

AirMagnet® Spectrum XT

User Guide



© 2009-2011 Fluke Corporation. All rights reserved.

AirMagnet® Spectrum XT User Guide.

This *User Guide* is furnished under license and may be used or copied only in accordance with the terms specified in the license. The content of this document is for information only and should not be construed as a commitment on the part of AirMagnet, Inc.

No part of this document may be reproduced, transmitted, stored in a retrievable system, or translated into any language in any form or by any means without the prior written consent of AirMagnet, Inc. Further, AirMagnet, Inc. reserves the right to modify the content of this document without notice.

AIRMAGNET, INC. SHALL NOT BE HELD LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THIS CONTENT.

AirMagnet® and AirWISE® are registered trademarks, and the AirMagnet logo is a trademark, of AirMagnet, Inc, a Fluke Networks company. All the other product names mentioned herein are trademarks or registered trademarks of their respective companies.

Fluke Networks
2575 Augustine Drive
Santa Clara, CA 95054
USA

Compiled in the United States of America. December 2011.

Documentation ID: ASXT-v301-USG-01-122011

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE AIRMAGNET SOFTWARE AND RETURN THE UNUSED AIRMAGNET SOFTWARE WITHIN THIRTY (30) DAYS TO THE PLACE WHERE YOU OBTAINED IT FOR A REFUND.

1. GRANT OF LICENSE.

Fluke Networks, a division of Fluke Electronics Corporation grants you a non-exclusive right to install and use the full version of the AirMagnet Software on a single computer at a time for use only with the MAC address of the Wi-Fi Card or Ethernet Interface or the unique identifier that you registered with Fluke Networks. The software and documentation accompanying this License whether on disk, in read only memory, on any other media or in any other form (the "AirMagnet Software") are licensed to you by Fluke Networks.

PLEASE NOTE: Activation of the AirMagnet Software requires a license key which Fluke Networks provides you. This license key is generated using the media access control ("MAC") address of either {a} a wireless network interface card (a "Wi-Fi Card") connected to your computer or {b} the Ethernet interface of your computer ("Ethernet Interface") or {c} identifiers of certain AirMagnet adapters. In certain cases, the Ethernet and/or Wi-Fi MAC address option may not be available. DURING THE INITIAL INSTALLATION OF THE AIRMAGNET SOFTWARE, YOU WILL BE REQUIRED TO CHOOSE TO LOCK THIS SOFTWARE LICENSE TO THE ETHERNET INTERFACE OF A SINGLE WINDOWS COMPUTER OR TO A SINGLE WI-FI CARD OR TO THE UNIQUE IDENTIFIER. THIS CHOICE IS PERMANENT AND CAN NOT BE CHANGED.

You acknowledge and agree that the AirMagnet Software is only authorized for use with the MAC address of the Wi-Fi Card or the Ethernet Interface of your computer or the unique identifier that you registered with Fluke Networks, the licensing mechanism of the AirMagnet Software prevents use of the AirMagnet Software with other MAC addresses or unique identifiers, and you will not in any way attempt to circumvent the licensing mechanism of the AirMagnet Software. You also acknowledge and agree that to ensure authorized use as described above, each time you use the AirMagnet Software, Fluke Networks may track the following information: your Ethernet and wireless addresses; unique identifier, user, system and domain names; date and time the AirMagnet Software launched; product serial number and serial key. Fluke Networks will not share this information with third parties except with third parties who perform services for it or if compelled by law, if necessary to protect and defend Fluke Networks rights or property or to act in an emergency to protect someone's safety.

2. TITLE, COPYRIGHT AND TRADEMARK.

Software is owned by Fluke Electronics Corporation and is protected by United States copyrights laws and international treaty provisions. Therefore you must treat the Software like any other copyrighted material. You own the media on which the AirMagnet Software is recorded but Fluke Network's and/or Fluke Networks' licensor(s) retain title to the AirMagnet Software. The AirMagnet Software in this package and any copies which this License authorizes you to make are subject to this License.

3. PERMITTED USES AND RESTRICTIONS.

This License does not allow the full version or the limited version of the AirMagnet Software to exist on more than one computer at a time. You may make one copy of the AirMagnet Software in machine-readable form for backup purposes only. The backup copy must include all copyright information contained on the original. Except as expressly permitted in this License, you may not decompile, reverse engineer, disassemble, modify, rent, lease, loan, sublicense, distribute or create derivative works based upon the AirMagnet Software in whole or part or transmit the AirMagnet Software over a network. For certain AirMagnet software products, you may be entitled to a "viewer-only" software license in addition to the full-version of the software to allow you to view information generated by the full-version software on a separate Windows computer.

You may not disclose any information relating to the performance or operation of the AirMagnet Software (including any benchmarking or other testing results) to any third party without Fluke Networks' express prior written consent. You may, however, transfer your rights under this License, provided that you transfer the related documentation, this License and a copy of the AirMagnet Software to a party who agrees to accept the terms of this License and destroy any other copies of the AirMagnet Software in your possession. You acknowledge that the AirMagnet Software contains or is provided with copyrighted software of Fluke Networks' suppliers as identified in associated documentation or other printed materials ("Third Party Software") which are obtained under a license from such suppliers. Your use of any Third Party Software shall be subject to and you shall comply with the applicable restrictions and other terms and conditions set forth in such documentation or printed materials. You may not use or otherwise export or re-export the AirMagnet Software except as authorized by United States law and the laws of the jurisdiction in which the AirMagnet Software was obtained. In particular, but without limitation, the AirMagnet Software may not be exported or reexported (i) into (or to a national or resident of) any U.S. embargoed country or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders. By using the AirMagnet Software, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

4. TERMINATION.

Your rights under this License will terminate automatically without notice from Fluke Networks if you fail to comply with any term(s) of this License.

PLEASE NOTE: If Fluke Networks discovers or has reason to believe that you have breached your obligations under this License, including but not limited to your unauthorized use of the AirMagnet Software, Fluke Networks reserves the right in its sole discretion to (1) disable your access to any copies of AirMagnet Software in your possession or under your control and (2) seek monetary damages against you up to the maximum amount permitted by law. In connection with any such breach or suspected breach, you will pay all costs, expenses and fees (including but not limited to reasonable attorneys' fees and auditing fees) incurred by Fluke Networks in its enforcement of this provision.

5. LIMITED WARRANTY.

Fluke Networks warrants the media on which the AirMagnet Software is recorded to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of original retail purchase. Fluke Networks does not warrant any downloading errors or that the Software will be error free or operate without interruption. Fluke Networks' entire liability and your exclusive remedy under this paragraph shall be, at Fluke Networks' option, a refund of the purchase price of the product containing the AirMagnet Software or replacement of the AirMagnet Software which is returned to Fluke Networks or an authorized representative with a copy of the receipt. This limited warranty is void if failure of the products has resulted from accident, abuse, or misapplication. Any replacement product will be warranted for the remainder of the 90 day original warranty period or 30 days, whichever is longer.

6. DISCLAIMER OF WARRANTY ON AIRMAGNET SOFTWARE.

Other than as provided in the Limited Warranty above, the AirMagnet Software is provided "AS IS" and without further warranty. FLUKE NETWORKS EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE AIRMAGNET SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE AIRMAGNET SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE AIRMAGNET SOFTWARE WILL BE CORRECTED. FURTHERMORE, FLUKE NETWORKS DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE AIRMAGNET SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY FLUKE NETWORKS OR A FLUKE NETWORKS AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL FLUKE NETWORKS BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Fluke Networks' total liability to you for all damages exceed the amounts paid by you hereunder.

8. GOVERNMENT END USERS.

AirMagnet Software is a "commercial item," "commercial computer software" and/or "commercial computer software documentation." Consistent with DFAR section 227.7202, FAR section 12.212 and other sections, any use, modification, reproduction, release, performance, display, disclosure or distribution thereof by or for the U.S. Government shall be governed solely by the terms of this License and shall be prohibited except to the extent expressly permitted by the terms of this License.

9. CONTROLLING LAW AND SEVERABILITY.

This License shall be governed by the laws of the United States and the State of Washington, U.S.A., without reference to its conflict of law principles. The United Nations Convention on the International Sale of Goods shall not apply to this License. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

10. COMPLETE AGREEMENT.

This License constitutes the entire agreement between the parties with respect to the use of the AirMagnet Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Fluke Networks.

Table of Contents

Software License Agreement	i
Chapter 1: Introduction	1
Product Overview	1
Main Features	1
Ability to Scan All 802.11 Frequency Bands	1
Spectrum Graphs	1
Real-Time FFT Graph	1
Spectrum Density Graph	1
Spectrogram Graph	1
Channel Power Graph	2
Channel Duty Cycle Graph	2
Non-WiFi Devices	2
Event Spectrogram	2
Interference Power	2
Channel Duty Cycle vs Time	2
Interference Power vs Time	2
WiFi Graphs	2
AP Signal Strength Graph	3
Top 10 APs by Speed Graph	3
Top 10 Active APs' Retry/CRC Graph	3
WiFi Devices Graph	3
Channel Occupancy Graph	3
Channels by Speed Graph	3
Channels by Media	3
Channels by Address	3
Channel Utilization Graph	3
Channel Signal/Noise Ratio	3
Channels by Retry/CRC	4
Auto Pattern Detection and Custom Device Classification	4
Find Device Tool	4
Instant Playback of Capture Data	4
Recording Live Capture Data	4
Auto Recording Capture Data	4
Saving Recorded Capture Data	5
Replaying Saved Capture Data	5
Remote XT Connection	5
Right-Click Menus	5
Right-Click to Copy and Paste	5
Right-Click to Save	5

System Requirements	6
Adapters	6
Laptop/Tablet PC	6
Netbook	6
Apple® MacBook® Pro.....	7
Fluke Networks OptiView® Series II/III Integrated Network Analyzer.....	7
Fluke Networks OptiView XG Network Analysis Tablet.....	7
Supported Wireless Network Adapters	8
AirMagnet Spectrum XT on Fluke Networks Optiview INA	8
Usability	9
MyTTouch Soft Keyboard	9
Right Mouse-Click Emulation.....	10
Device Ageout	10
Chapter 2: Getting Started	11
Chapter Summary	11
Preparing for Software Installation	11
Keeping Your Serial Number and Serial Key Handy	11
Having Live Internet Access	11
Installing AirMagnet Spectrum XT from a CD.....	11
Installing the USB Spectrum Drivers	12
Installing AirMagnet Spectrum XT	12
Installing Your Software License File	13
Downloading and Installing the License File over the Internet.....	13
Installing the License File Locally	16
Product Registration.....	16
Technical Support	17
Contact Customer Support.....	18
AirWISE Community	18
Chapter 3: AirMagnet Spectrum XT User Interface	19
Chapter Summary	19
AirMagnet Spectrum XT Screen Options	19
AirMagnet Spectrum XT Major UI Components	19
Toolbar.....	21
Spectrum-WiFi Summary	24
Channel Summary	24
Device List.....	25
Channel Devices.....	26
Graph Window.....	26
Channel Scan Indicator	27

Chapter 4: Menus and Tools	29
Chapter Summary.....	29
Selecting a Radio Band.....	29
Add View	30
Managing Live Data Capture.....	31
Pausing and Resuming Live Capture	31
Instantly Playing Back Captured Data	31
Recording a Live Capture Data	32
Saving Recorded Data to File	32
Opening a Capture Data File.....	33
Resetting Collected Data.....	33
Configuring AirMagnet Spectrum XT Settings	33
Configuring WiFi and Spectrum Parameters	33
Selecting Another WiFi Driver.....	36
Specifying Band Settings.....	36
Modifying Display Options.....	37
Specifying Record Settings	38
Virtual AP Grouping	40
Auto Group Rules.....	41
Manual Group Rules	41
Integration of AirMagnet Spectrum XT with SNMP Management Stations	42
Remote Spectrum Analysis	44
Using Easy View Options	45
Using a Default Easy View Option	45
Creating a Custom View Option	46
Deleting a Custom View Option	47
Saving Current View	47
Automatically Saving Current View.....	48
Manually Saving Current View	48
Copying a Graph into Other Applications.....	48
Saving Screen Data as Image Files	49
Dwell Time (FFT Max Data Sampling Duration).....	50
AirMagnet Spectrum XT Report.....	50
Chapter 5: Auto Pattern Detection and Custom Device Classification	51
Chapter Summary.....	51
Auto Pattern Detection.....	51
Best Practices	53
Custom Device Classification Manager.....	54
Verification.....	57
Export/Import Custom Signatures	58

Custom Signature During File Playback	60
Chapter 6: Analyzing Spectrum Data.....	61
Chapter Summary	61
Spectrum Graph Options	61
Real Time FFT	62
Channel Duty Cycle Overlay on FFT Graph	64
Setting FFT Graph Parameters	64
Spectrum Density Graph	67
Viewing AP Signal Strengths Across Frequency Range	68
Configuring Spectrum Density Plot Parameters	68
Spectrogram Graph	71
Configuring Spectrogram Graph Parameters	71
Channel Power	73
Channel Power Types	74
Configuring Channel Power Graph Parameters	74
Channel Duty Cycle.....	76
Configuring Channel Duty Cycle Graph Parameters	77
Non-WiFi Devices	78
Event Spectrogram.....	80
Configuring Event Spectrogram.....	80
Interference Power.....	81
Configuring the Interference Power Display	82
Channel Duty Cycle vs Time.....	83
Configuring Channel Duty Cycle vs Time.....	84
Interference Power vs Time.....	85
Configuring the Interference Power vs Time Graph	86
BlueSweep Integration	87
Additional Bluebooth Analysis.....	87
Chapter 7: Analyzing WiFi Data	89
Chapter Summary	89
WiFi Graph Options	89
WiFi Devices Graph.....	90
AP Signal Strength Graph	92
Channel Occupancy Graph	94
Channels by Speed.....	95
Channels by Media	96
Channels by Address.....	97
Channel Utilization.....	99
Top 10 APs by Speed	100
Top 10 Active APs' Retry/CRC	101

Channel Signal/Noise Ratio.....	103
Channels by Retry/CRC.....	103
Chapter 8: Finding Devices	105
Chapter Summary.....	105
Find Device Screen UI Components	105
Event Log	106
Device Details.....	106
Device Pattern	108
Find Device Tool.....	108
Device Description.....	109
Physically Locating a Device on the Network.....	110
Best Practices	110
With Omni-directional Antenna.....	110
With Directional Antenna.....	110
Chapter 9: Radar Detection Tool.....	113
Chapter Summary.....	113
Introduction	113
AirMagnet Spectrum XT Radar Detection Tool	113
Impact on 802.11 WLAN.....	114
Recommended Courses of Action	114
Radar Detection Tool UI Components.....	115
Using the Radar Detection Tool.....	117
Chapter 10: Device Detection.....	119
Chapter Summary.....	119
Non-WiFi (Spectrum) Devices	120
Bluetooth Devices	120
RF Spectrum Pattern.....	120
Impact on 802.11b/g WLAN.....	121
Recommended Courses of Action	121
Digital Cordless Phones	121
RF Spectrum Pattern.....	122
Impact on 802.11 WLAN.....	123
Recommended Courses of Action	123
Analog Cordless Phones	124
RF Spectrum Pattern.....	124
Impact on 802.11 WLAN.....	124
Recommended Courses of Action	125
Microwave Ovens	125
RF Spectrum Pattern.....	125

Impact on 802.11b/g WLAN.....	126
Recommended Courses of Action.....	126
Wireless Cameras.....	126
RF Spectrum Pattern.....	127
Impact on 802.11b/g WLAN.....	127
Recommended Courses of Action.....	127
Baby Monitors	128
RF Spectrum Pattern.....	128
Impact on WiFi Networks	128
Recommended Courses of Action.....	128
RF and Narrowband Jammer	129
RF Spectrum Pattern.....	129
Impact on WiFi on WiFi Networks	130
Recommended Course of Actions	130
Digital Video Monitors	131
RF Spectrum Pattern.....	131
Impact on 802.11b/g WLAN.....	131
Recommended Courses of Action.....	131
Zigbee	132
RF Spectrum Pattern.....	132
Impact on 802.11b/g WLAN.....	133
Recommended Courses of Action.....	133
Motion Detector	134
RF Spectrum Pattern.....	134
Impact on 802.11 WLAN.....	134
Recommended Courses of Action.....	135
RF Signal Generator.....	135
Recommended Courses of Action.....	135
Impact on 802.11 WLAN.....	135
Recommended Course of Action.....	135
Non-Bluetooth Wireless Mouse.....	136
RF Spectrum Pattern.....	137
Impact on 802.11 WLAN.....	138
Recommended Course of Action.....	138
Wireless Game Controllers.....	139
RF Spectrum Pattern.....	139
Impact on 802.11b/g WLAN.....	140
Recommended Courses of Action.....	140
Frequency-hopping Spread Spectrum devices.....	140
Introduction	140
RF Spectrum Pattern.....	140
Impact on 802.11 WLAN.....	141
Recommended Courses of Action	141

WiFi Devices	142
802.11 a/g/n APs.....	142
RF Spectrum Pattern.....	143
Impact on WiFi Networks	143
Recommended Courses of Action	144
802.11b APs.....	144
RF Spectrum Pattern.....	145
Impact on WiFi Networks	145
Recommended Courses of Action	146
 Abbreviations & Acronyms	 147
 Glossary	 149
 Index	 159

Chapter 1: Introduction

Product Overview

AirMagnet Spectrum XT is a brand-new WiFi troubleshooting and optimization tool from AirMagnet, Inc. designed to provide WiFi network professionals with a clear and concise view into their wireless network environment. AirMagnet Spectrum XT's power reaches far beyond its sleek and intuitive design, because it includes the option to complement spectrum analysis with WiFi packets and traffic analysis, using an optional second WiFi card. This allows users to directly connect spectrum information to the real performance of their wireless APs and channels. The software brings everything together in a single, clean interface that ensures that users can easily see the information that they need without digging through pages of data.

Main Features

AirMagnet Spectrum XT has the following main features:

Ability to Scan All 802.11 Frequency Bands

AirMagnet Spectrum XT has the capability to capture live spectrum and WiFi data in the wireless network and display them in real time on the screen, assuming the user has an AirMagnet-supported wireless network adapter installed and enabled at the same time. To make it easier for the user to focus on certain part of the 802.11 radio spectrum, AirMagnet Spectrum XT offers six band options: 2.4 GHz, 4.9 GHz, 5 GHz Lower, 5 GHz Middle, 5 GHz Upper, and Mixed which includes all options other than 4.9 GHz. The user can choose any of these band options from the Band menu in the toolbar.

Spectrum Graphs

AirMagnet Spectrum XT can display spectrum data it captures in a variety of spectrum graphs, each allowing the user to analyze the spectrum data from a unique perspective. The spectrum graphs are:

Real-Time FFT Graph

The Real-Time FFT (Fast Fourier Transformation) graph displays in real time the current, average, and maximum FFT readings. It shows the RF power as a function of radio frequency. The user can fine-tune the graph by modifying certain parameters of the graph such as the type of data to be graphed, power settings, frequency range, etc.

Spectrum Density Graph

The Spectrum Density graph shows the popularity of a particular frequency/power reading over time. It can also display the signal strength of selected APs across the corresponding frequency ranges used by the APs.

Spectrogram Graph

The Spectrogram graph shows the distribution (sweep) of energy across the radio band over time and changes in frequency use and the duration of such changes.

Channel Power Graph

The Channel Power graph shows the current and maximum (aggregated) channel energy. The graph can display either Envelope Power or Integrated Power. The former refers to the highest power reading and the latter shows the total summation of power readings over a specific bandwidth.

Channel Duty Cycle Graph

The Channel Duty Cycle graph shows the percentage of the time that the average power in the channel is greater than 20 dBm above the noise floor.

Non-WiFi Devices

The Non-WiFi Devices table lists all non-WiFi devices whose spectrum information has been detected by the application, along with some key data about each device. The devices are organized by category which includes Bluetooth devices, microwave ovens, cordless phones, baby monitors, FR Jamters, and wireless cameras.

Event Spectrogram

The Event Spectrogram provides a visual presentation of real-time information about events (device detections) that the application has detected in the network. Each detection is an event which is represented by a colored line. The color of the line indicates the signal strength of the device being detected. If more detections are made of the same device as the application sweeps the spectrum, more lines will be stacked on top of the line of the initial detection. As a result, a thick color band will result. The height of the color band indicates the (length of time in seconds the device has been detected. It stops increasing when the device becomes inactive (meaning that the device has not been detected for a minute). The width of the line/band indicates the channels or frequencies being affected by the device. If the device is a frequency-hopping device, then the line/band may extend sideways as the device hops from one channel to another.

Interference Power

The Interference Power graph displays the average power readings of interfering devices on the selected channel or channels.

Channel Duty Cycle vs Time

The Channel Cycle vs. Time graph is a trending chart which shows the average power in the channel is above the noise floor over a specific period of time.

Interference Power vs Time

The Interference Power vs. Time graph is a trending chart which shows the maximum average power readings of interfering devices operating on the selected channel over a specific period of time.

WiFi Graphs

AirMagnet Spectrum XT offers many WiFi graphs to complement its spectrum capability. These WiFi graphs offer critical data about the performance of a WiFi network. The nine WiFi graphs are:

AP Signal Strength Graph

The AP Signal Strength graph identifies and displays up to three APs with the strongest signal strengths on each available channel in the selected radio band.

Top 10 APs by Speed Graph

The Top 10 APs by Speed graph displays up to 10 APs with the fastest transmission speeds as well as the data rate or rates used by each of the top APs. Each bar represents an AP.

Top 10 Active APs' Retry/CRC Graph

The Top 10 Active APs' Retry/CRC graph shows up to 10 APs with the most Retry or CRC rates on each of the available channels for the selected media. The X-axis lists all available channels and the Y-axis shows the percentages or retry and/or CRC rates.

WiFi Devices Graph

The WiFi Devices graph (table) displays all WiFi devices detected on the WiFi network. The devices are organized three categories, which are Station, AP, and Phone.

Channel Occupancy Graph

The Channel Occupancy graph allows the user to visualize all the available channels for the selected radio band and shows which AP or APs are occupying what channel. It also indicates the center frequency used by an AP and channels affected by RF interference caused by the AP. The information helps the user make well-informed decisions on AP channel allocation to optimize their performance.

Channels by Speed Graph

The Channel by Speed graph displays the amount of data in kilobytes sent at each transmission rate on each of available channel for the selected radio band.

Channels by Media

The Channel by Media graph shows the amount of data (in kilobytes) transmitted by data type (i.e., 802.11a, b, g, and n) on each available channel for the selected radio band.

Channels by Address

The Channel by Address graph shows the amount (in kilobytes) of data transmitted by each address type (i.e., broadcast, unicast, or multicast) on each available channel for the selected radio band.

Channel Utilization Graph

The Channel Utilization graph shows the percentage of bandwidth being used on each channel and the breakdown of the utilization by data transmission rate.

Channel Signal/Noise Ratio

The Channel SNR graph shows the signal-to-noise ratio on all available channels in the selected radio band.

Channels by Retry/CRC

The Channels by Retry/CRC graph allows the user to quickly assess which channels are experiencing high levels of Retry or CRC packets.

Auto Pattern Detection and Custom Device Classification

Auto Pattern Detection and Custom Device Classification enables users to identify, classify, and analyze interferers beyond those devices included in the software package.

- **Auto Pattern Detection:** The system identifies and lists persistent RF patterns that do not match its database of interferers. The user may name and save the pattern in order to have it show up as a named interferer in the future when that pattern is detected.
- **Custom Device Classification:** The user may create a custom signature of an RF pattern in order to have it show up as a named interferer in the future when that pattern is detected.

Find Device Tool

The Find Device tool enables the user to find any device (WiFi or non-WiFi) that the application has detected. You can launch the Find Device screen by clicking the **Find Device** button. Once on the Find Device screen, you can select the device of interest and use the application to physically locate the device on the network. The screen shows in real time the signal strength (if the device in question is a non-WiFi device) or signal strength and noise level (if it is a WiFi device). You can also turn on the audio feature to assist in locating the device: the closer you approach the device, the louder it ticks.

Instant Playback of Capture Data

The instant playback feature allows the user to revisit something they have noticed for the last two minutes on the live screen. It is very useful when the user wants to take a closer look at what has caught their attention at the first glance. The user can save to a file the data that they revisited and play back the data within the application by opening that file. To switch to instant playback mode, simply click the **Switch to Instant Playback** button on the toolbar.

Recording Live Capture Data

This feature allows the user to record live capture data the application captures to the hard drive of the PC. The user can interrupt the recording at any time by clicking and save the recorded data to a .amt file. The length of the recording depends on the **Max Live Capture Streaming File Size [MB]** the user has configured. The application will stop recording once the limit has been reached. Upon completion of the recording, the user will be prompted to save the recorded data.

Auto Recording Capture Data

By default, when launching AirMagnet Spectrum XT, data is automatically recorded. The user may stop the data recording by clicking on the Stop button on the toolbar. To switch to instant playback mode, simply click the **Switch to Instant Playback** button on the toolbar.

Saving Recorded Capture Data

This feature allows the user to save to a .amt file the live data they have recorded. To save recorded data, the user must stop recording data or let the application automatically stop recording once the Max **Live Capture Streaming File Size [MB]** is reached. The data saved in a .amt file can then be played back in the application for analysis.

Replaying Saved Capture Data

This feature allows the user to replay recorded data that has been saved in a .amt file. Once the file is opened, it will automatically replay, allowing the user to revisit the RF data captured in the file.

Remote XT Connection

The Remote XT Connection option enables the user to view remote, real-time data in their local Spectrum UI. It does this by connecting to a remote machine running an AirMagnet Spectrum Analyzer card.

To enable the Remote XT Connection option:

First, on the remote machine, establish a security password.

- 1) From the Toolbar, choose File>Remote XT Connection>Remote Access Authentication.
- 2) Type in a password. The password allows only numerical and special characters up to 16 characters in length.
- 3) Click **OK**.

Second, on the local machine, establish a connection to the remote machine.

- 1) From the Toolbar, choose File> Remote XT Connection>Connect to Remote Host.
- 2) Configure the IP address and port for the remote machine.
- 3) Type the security password previously created on the remote machine.
- 4) Click **Connect**.

Right-Click Menus

AirMagnet Spectrum XT comes with right-click menus for the graph window, which contain two options:

Right-Click to Copy and Paste

The feature allows the user to easily copy any graph displayed on the screen and paste it into any software document that supports copy-and-paste operation.

Right-Click to Save

The feature allows the user to save any graph shown on the screen as an image file in any of the following four image formats:

- .PNG
- .BMP

- .JPG
- .GIF

System Requirements

Minimum System requirements for installing and operating AirMagnet Spectrum XT vary, depending on the hardware platforms being used:

Note: 64-bit Operating System supported on Windows 7 for certain wireless adapters. Please refer to supported adapter list for more details.

Adapters

- AirMagnet Spectrum USB adapter (required for viewing RF spectrum data and classifying non Wi-Fi sources of interference)
- Optional AirMagnet-supported Wi-Fi adapter* (required for additional Wi-Fi analysis)
- Optional Windows-compatible Bluetooth adapter (required for enhanced Bluetooth interferer information)

Laptop/Tablet PC

- Microsoft® Windows XP™ Professional (SP3), Microsoft® Windows 2003 Server, Microsoft® Windows 7 Enterprise/Professional/Ultimate, Microsoft® Windows Vista™ Business or Ultimate (SP2) or Tablet PC Edition 2005 (SP3), Microsoft Windows 2008 R2 Standard Edition (for spectrum data).

Note: 64-bit operating system supported on Microsoft® Windows 7 only.

- Intel® Core™ 2 Duo 2.00 GHz or higher
- 1 GB RAM required (92 GB recommended)
- 150 MB of available hard drive space
- Microsoft .NET Framework 2.0
- Optional Windows-compatible Bluetooth adapter (required for enhanced Bluetooth interferer information)

Netbook

- Microsoft® Windows XP™ Home, Microsoft® Windows 7 Home Premium, Microsoft® Windows 7 Starter
- Intel® Atom N270/1.6 GHz CPU or N470 Processor (1.83 GHz, 667MHz FSB)
- Microsoft .NET Framework 2.0
- 1 GB memory (2 GB recommended)

- Optional Windows-compatible Bluetooth adapter (required for enhanced Bluetooth interferer information)

Apple® MacBook® Pro

- MAC OS X Leopard™, MAC OS X Snow Leopard™ [running Windows XP™ PRO (SP3) or Microsoft® Windows 7 Professional/Enterprise/Ultimate using Boot Camp®; Parallels Desktop® or VMWare Fusion® running Windows XP PRO (SP3) or Microsoft® Windows 7 Professional/Enterprise/Ultimate]
- Intel 2.2 GHz Core 2 Duo or higher
- Microsoft.NET Framework 2.0
- 1 GB memory (2 GB recommended)
- Optional Windows-compatible Bluetooth adapter (required for enhanced Bluetooth interferer information)

Fluke Networks OptiView® Series II/III Integrated Network Analyzer

- Microsoft® Windows XP™ Professional (SP3)
- Intel® Pentium M 600 MHz
- 512 MB memory
- Microsoft .NET Framework 2.0
- For additional Wi-Fi analysis, Wi-Fi CardBus adapters supported include: Airmagnet 802.11 a/b/g/n Wireless PC card, Fluke Networks 802.11 a/b/g/n, or Fluke Networks 802.11 a/b/g

Note: 1] See website [http://airmagnet.com/products/spectrum_xt/?td=supported_adapters] for a complete list of AirMagnet Spectrum XT supported adapters.

2] Optional Windows-compatible Bluetooth adapter not supported.

Fluke Networks OptiView XG Network Analysis Tablet

- Microsoft Windows 7, Professional, SP1
- Intel Pentium 1.2 GHz
- 4 GB memory
- 128 GB removable solid state drive
- 2 internal Atheros®-based 802.11a/b/g/n adapters
- 1 internal RF spectrum adapter
- 3 USB ports
- 1024 x 768 touch display

Supported Wireless Network Adapters

An AirMagnet-supported wireless network adapter is required in order to capture and display WiFi data in AirMagnet Spectrum XT. For a complete, up-to-date listing of AirMagnet-supported wireless adapters, visit http://www.airmagnet.com/support/supported_adapters/.

AirMagnet Spectrum XT on Fluke Networks Optiview INA

Fluke Networks' OptiView® Integrated Network Analyzer is a powerful, portable, all-in-one network analysis solution that provides the vision and capabilities to help you deploy new technologies and applications, manage and validate infrastructure changes, solve network and application performance issues, as well as secure the network from internal threats.

Today's networks may be more stable, but certainly not static. Management and users are constantly demanding new technologies, new services, and better performance which inevitably require infrastructure changes, deployment of new, emerging applications, and dealing with security issues. In the midst of all this, you need to control IT costs and minimize disruption to your organization. That means you need to be able to clearly see all aspects of your network to accurately assess the overall impact. The more your network changes, the more you will need to improve visibility and control.

The OptiView analyzer improves your visibility into your 10/100/1000 copper and optical networks through:

- Advanced discovery techniques – Automatically begins to discover devices on the network e.g., switches, routers, wireless controllers, VoIP devices. IT staff can immediately see what's on the network and problems associated with those devices.
- Traffic analysis – Provides real-time statistics for traffic on the wire enabling the user to understand how the network resources are being used.
- Application traffic analysis – Automatically discover all IPv4 and IPv6 protocols and sub protocols from layer 1 – 7 enabling IT staff to identify applications utilizing link bandwidth as well as top hosts and conversations.

You can expand the power of the OptiView analyzer by adding visibility into your local 802.11abgn networks with AirMagnet® WiFi Analyzer PRO, Survey PRO, and AirMagnet Spectrum XT products.



Figure 1-1: AirMagnet Spectrum XT on the OptiView INA

Usability

The sections below detail some of the features specific to the OptiView machine designed to enhance the user experience and make AirMagnet Spectrum XT easier to use.

MyTTouch Soft Keyboard

Any window in which the user is expected to enter text should automatically open the MyTTouch Soft Keyboard, which allows the user to provide text input. In cases where the user wishes to access the keyboard and it is not displayed automatically, there should be a small keyboard button (🖱️) in the upper right-hand corner of the window. Tap the MyTTouch button to bring up the soft keyboard and tap the keys as needed. See Figure 1-2.



Figure 1-2: OptiView MyTTouch Soft Keyboard Interface

Right Mouse-Click Emulation

In order to access the right-click menu used by many AirMagnet Spectrum XT screens, tap and hold until the menu appears (note that it is important that the user not move the cursor after the initial tap until the menu appears). Alternatively, users can also tap the mouse icon in the System Tray (shown in Figure 1-3) to specify that the next tap will emulate a right-click.



Figure 1-3: The OptiView Taskbar

Device Ageout

In order to enhance application performance for the OptiView INA, AirMagnet Spectrum XT automatically incorporates a mechanism to “age out” devices when it is running on the INA platform. A device that is aged out is effectively removed from the active device list and purged from memory. This process will apply to devices when the following two requirements are met:

- The device has been inactive for over 1 hour.
- The total number of **non-wifi** devices is greater than 50.

Chapter 2: Getting Started

Chapter Summary

This chapter discusses the procedures for installing AirMagnet Spectrum XT. It covers the following topics:

- Preparing for software installation
- Installing AirMagnet Spectrum XT from a CD
- Registering Your AirMagnet Spectrum XT
- Seeking Technical support

Preparing for Software Installation

This section contains instructions on the installation of the AirMagnet Spectrum XT software. To ensure that your software installation proceeds smoothly, it is strongly recommended that you read these instructions carefully before starting the installation. Failure to read these instructions may cause unnecessary delay in the installation process and even hinder you from fully utilizing the application.

Keeping Your Serial Number and Serial Key Handy

The entire software installation may require the downloading of the software license from AirMagnet's website, which occurs when you restart the computer upon the completion of the installation. To download the software license, you will be prompted to provide a valid serial number and serial key for the software. It is strongly recommended that you have your software's serial number and serial key handy at the time of installation. Both the serial number and the serial key are printed on a sticker attached to your software certificate inside the product package.

Having Live Internet Access

Because you may need to download the software license and register your product from AirMagnet's website, you must have a live Internet connection, in addition to a valid serial number and serial key, for the application to complete the process.

Installing AirMagnet Spectrum XT from a CD

This section discusses installing AirMagnet Spectrum XT from a CD. You should follow these instructions to install the software if you have purchased the AirMagnet Spectrum XT software package, which includes the software CD.

To start the installation process, insert the AirMagnet Spectrum XT CD in the PC's CD-ROM drive. The installation menu should appear automatically. See Figure 2-1.

*If the installation fails to start automatically, browse to the CD-ROM drive on your computer and double-click the **autorun.exe** file inside the folder.*

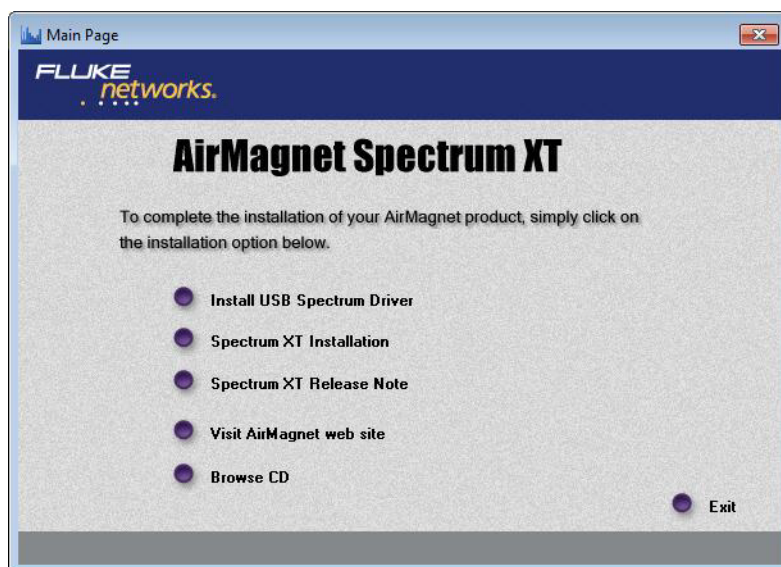


Figure 2-1: AirMagnet Spectrum XT Autorun

The Autorun menu allows the user to install the components of AirMagnet Spectrum XT as well as access product documentation. The following sections will go through the basic process of installing the components of AirMagnet Spectrum XT.

Installing the USB Spectrum Drivers

In order to ensure that the installation proceeds smoothly, it is strongly recommended that the user install the drivers for the AirMagnet spectrum adapter prior to installing AirMagnet Spectrum XT.

To install the drivers for the spectrum USB adapter:

- 1) From the Autorun menu, click **Install USB Spectrum Driver**.
- 2) Follow the instructions provided in the installation and click **Finish** to close the installation wizard.
- 3) Reboot the machine when prompted to complete the installation.

Installing AirMagnet Spectrum XT

After the USB driver installation has been completed, the machine is ready to have the AirMagnet Spectrum XT application installed.

To install AirMagnet Spectrum XT:

- 1) From the Autorun menu, click **Spectrum XT Installation**. The installation wizard appears.
- 2) Click **Next** to view the AirMagnet Inc. Software License Agreement.
- 3) Check the **I accept the terms of the license agreement** radio button and click **Next**.
- 4) Specify an installation path and click **Next**.
- 5) Click **Install** to begin the installation.
- 6) After the procedure has completed, click **Finish** to exit the install wizard.

Installing Your Software License File

When you launch AirMagnet Spectrum XT for the first time after installation, you will be prompted to install your software license file, which is required for activating and operating the software. Depending on your own circumstance, you can either download the license file online from AirMagnet's website or browse for the license file locally (if you already have a valid license file stored on your computer or network) and then install it. The following two sections provide detailed instructions on how to install the license file under each of the circumstances.

Downloading and Installing the License File over the Internet

The following instructions apply if you install AirMagnet Spectrum XT for the first time and/or do not yet have a valid license file stored on your computer or network. You must have a valid serial number and serial key as well as live Internet access, in order to use this option.

To download and install your software license file online:

- 1) From the desktop of your laptop computer, click **Start>All Programs>AirMagnet Spectrum XT>Spectrum XT**. The following message appears on screen. See Figure 2-2.

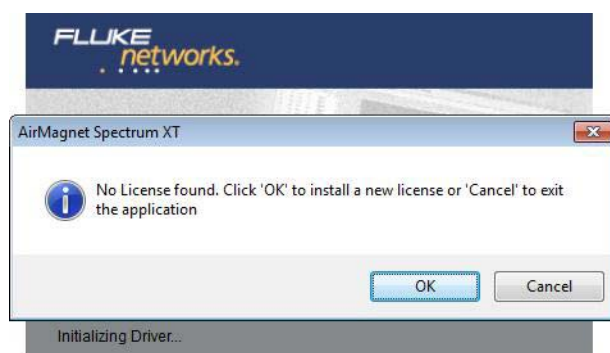


Figure 2-2: Installing software license

- 2) Click **OK**. The following screen appears. See Figure 2-3.

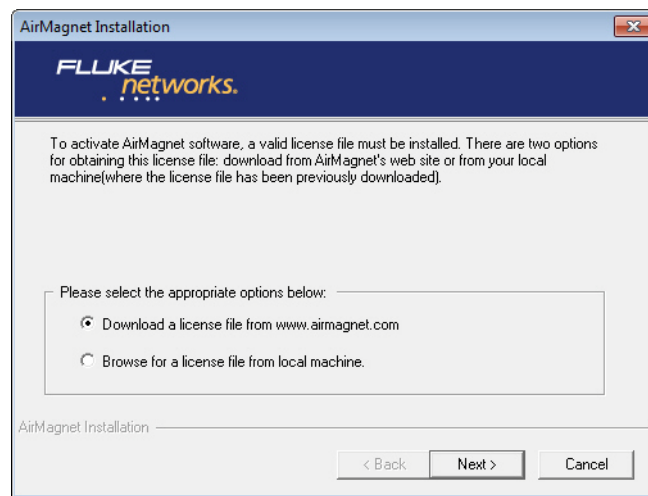


Figure 2-3: Entering your serial number and serial key

- 3) Select **Download a license file from www.airmagnet.com** and click **Next**. The following screen appears. See Figure 2-4.

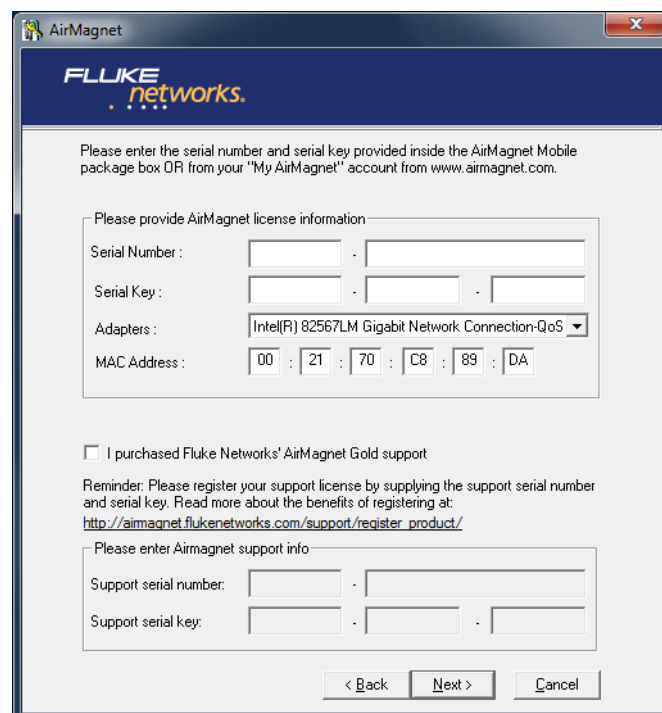


Figure 2-4: Downloading the license file online

- 4) Enter your software's serial number and serial key.

- 5) If you have AirMagnet Gold Support for this product, check the box and enter the support contract serial number and serial key.
- 6) Click **Next**.

*The Adapter and USB Serial Number fields are greyed out by default, but they will be automatically populated once you have entered the correct serial number and serial key. Once you click Next after you have entered a valid serial number and serial key, the application will download the license file from AirMagnet's website and install it on your computer at **C:\Program Files\AirMagnet Inc\Spectrum XT**. It is strongly recommended that you back up your license file at a safe location, for you need your license file if you ever want to reinstall AirMagnet Spectrum XT. Also, once the license is installed, the AirMagnet Web page will automatically open on the screen. You can either register the product right away using the Product Registration link on the Web page or close the Web page. It is strongly recommended that you register your product because registration is required for access to technical support, product update and upgrade, and other registration-only privileges. After you have closed the AirMagnet Web page, you may see a warning message similar to the one shown in Figure 2-5, depending on the anti-virus software installed on the PC.*

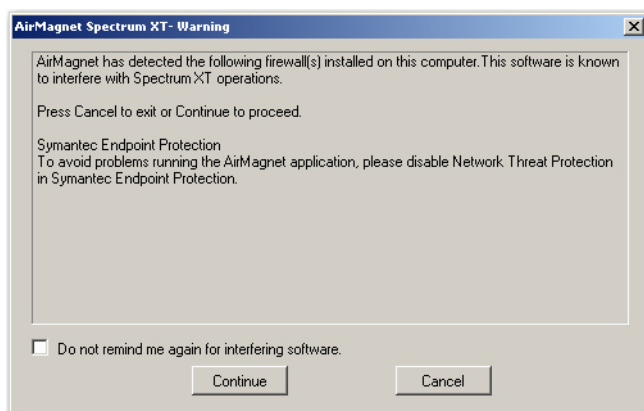


Figure 2-5: A firewall warning message

- 7) If prompted by a message similar to that in Figure 2-5, click **Continue**. AirMagnet Spectrum XT starts momentarily.

*A warning message like the one shown in Figure 2-5 appears whenever you launch the application. We recommend that you disable the firewall in your anti-virus software installed on the PC before you click the **Continue** button in the warning message. The application may not function properly if you do not have the firewall disabled. Clicking the **Cancel** button will abort the launching of the application.*

Installing the License File Locally

The following instructions apply if you already have a valid AirMagnet Spectrum XT license file stored locally, either on your computer or your network.

To install your software license file locally:

- 1) Repeat Steps 1 through 2 in the previous section until the License Download screen appears.
- 2) Select **Browse for a license file from local machine** and click **Next**. You will be prompted to enter the location of the license file.
- 3) Click **Browse** to browse for the license file and click **Open**.
- 4) Click **Next** to continue with the installation.

Once the license is installed, the AirMagnet Web page will automatically open on the screen. You can either register the product right away using the Product Registration link on the Web page or close the Web page. It is strongly recommended that you register your product because registration is required for access to technical support, product update and upgrade, and other registration-only privileges. After you have closed the AirMagnet Web page, you'll see a warning message similar to the one shown in Figure 2-5, depending on the anti-virus software installed on the PC.

- 5) Disable the firewall application being identified and then click **Continue**. AirMagnet Spectrum XT starts momentarily.

*A warning message like the one shown in Figure 2-5 appears whenever you launch the application. We recommend that you disable the firewall in your anti-virus software installed on the PC before you click the **Continue** button in the warning message. The application may not function properly if you do not have the firewall disabled. Clicking the **Cancel** button will abort the launching of the application.*

Product Registration

Towards the end of license file installation, the AirMagnet Product Registration Web page will appear. You can either register your product now by following the instructions on the screen or decline the registration by closing the Web page. However, because registering your AirMagnet Spectrum XT will ensure your eligibility for product support and access to information on product upgrades and other benefits, it is strongly recommended that you register your product at your earliest convenience.

You must register your product in order to receive product support.

To register your AirMagnet Spectrum XT:

- 1) Follow the instructions on the AirMagnet Product Registration Web page to register your AirMagnet Spectrum XT. See the illustration in Figure 2-6.

SUPPORT

- AirMagnet Support
- Training
- Online Training
- Knowledge Base
- Supported Adapters
- MAC Address Reset
- Product Registration

Product Registration

It is **highly recommended** that you register your AirMagnet software from this website. By registering your purchase you are entitled to a free MyAirMagnet.com account with the following benefits:

- Users can download software updates/upgrades to the software when available
- Access product documentation (FAQs, best practices, release notes, user guides, etc.)
- Download wireless adapter drivers
- Access technology notes/white papers
- Access to AirMagnet forums

Follow the steps below to register your AirMagnet product.

Step 1: Check your license, if you have a serial number that starts with "S", for example S4015-xxxxxx, this is your Support Serial number, you will be presented an opportunity to register your support after you have completed product registration. Support registration will be presented in your MyAirMagnet account. Registered Products/Downloads->Your Product->Register Support Contract.

Step 2: Enter the product serial number in the space below:

For new products, the serial number/key can be found on the Software License Certificate in the packaging, e.g., "A1150-04080001". Make sure to enter the number exactly as it appears on the label.

Note for older products: those serial numbers that do not start with "Axxx-" (e.g., "02480320"). Please contact Tech Support for product registration.

Important Note About Your MAC Address and Licensing:
As part of the end user license agreement (EULA), all AirMagnet software must be licensed to a specific MAC address. This can be the MAC address of the wireless adapter you plan to use or the internal wired Ethernet MAC address of the PC where you will run the AirMagnet software.

☐ I would like to register the serial number with a MAC Address
(Please check if you know the MAC address you want to license to. If you are unsure of the MAC Address you wish to license to, simply skip this and you will be allowed to choose the appropriate MAC address later during the AirMagnet software installation)

Step 3: Select one of the following:

☐ I currently have a MyAirMagnet account.

☒ I do not have a MyAirMagnet account.

NEXT

Figure 2-6: AirMagnet Product Registration page

If you prefer to register your AirMagnet Spectrum XT at a later time, you can open the same Product Registration Web page using the Web address http://www.airmagnet.com/support/register_product/ and then following the instructions on the screen to complete the registration.

Technical Support

Fluke Networks' Gold Support is our comprehensive support and maintenance program that offers expanded coverage for all AirMagnet products.

Benefits of the Gold Support program include:

- **Access to live 24 X 7 technical support**
 - Highly trained technical experts to help with product installation, configuration, best practices & troubleshooting on call 24 hrs a day including weekends and through the night.
 - Multilingual technical support team.

- **Free software updates/upgrades (new features and product enhancements) when available**
- **Hardware support, repair and replacement for AirMagnet products***
 - * Must meet terms and conditions as defined in the hardware warranty
- **Free access to “AirMagnet Certified Professional” web-based training for certain AirMagnet products**
- **MAC Address Reset assistance**

Contact Customer Support

- Navigate to http://www.airmagnet.com/my_airmagnet/ and log in to MyAirMagnet to access the “Exclusive” Gold-member only phone numbers for your region.
- Submit a support request.
- Send email to support@AirMagnet.com.

AirWISE Community

From the help menu, users can directly link to the AirWISE Community <http://www.airwisecommunity.com> created by AirMagnet for wireless experts. The AirWISE Community includes discussion forums, blogs and additional resources for the security, performance and compliance of wireless networks.

Chapter 3: AirMagnet Spectrum XT User Interface

Chapter Summary

This chapter discusses the major components of AirMagnet Spectrum XT's user interface. It describes what they are and how they can be used in analyzing spectrum and/or WiFi data that are captured on your network. It covers the following topics:

- AirMagnet Spectrum XT Screen Options
- AirMagnet Spectrum XT Major UI Components
- Toolbar
- Channel Summary
- AP List
- Channel Usage
- Graph Window
- Channel Scan Indicator

AirMagnet Spectrum XT Screen Options

AirMagnet Spectrum XT has two major screen options, represented by two buttons in the lower-left part of the application's user interface:

-  **Spectrum-WiFi Summary** - presents detailed RF spectrum information about all WiFi and non-WiFi devices detected in the network.
-  **Find Device** - contains tools for locating devices (WiFi or non-WiFi) that the application has detected.

By default, the Spectrum-WiFi Summary screen opens when the application is started. You can toggle between these two screen options using these buttons.

AirMagnet Spectrum XT Major UI Components

AirMagnet Spectrum XT has only one major user interface which shows various spectrum and/or WiFi data it captures in one single screen. Figure 3-1 highlights the AirMagnet Spectrum XT's major UI components.

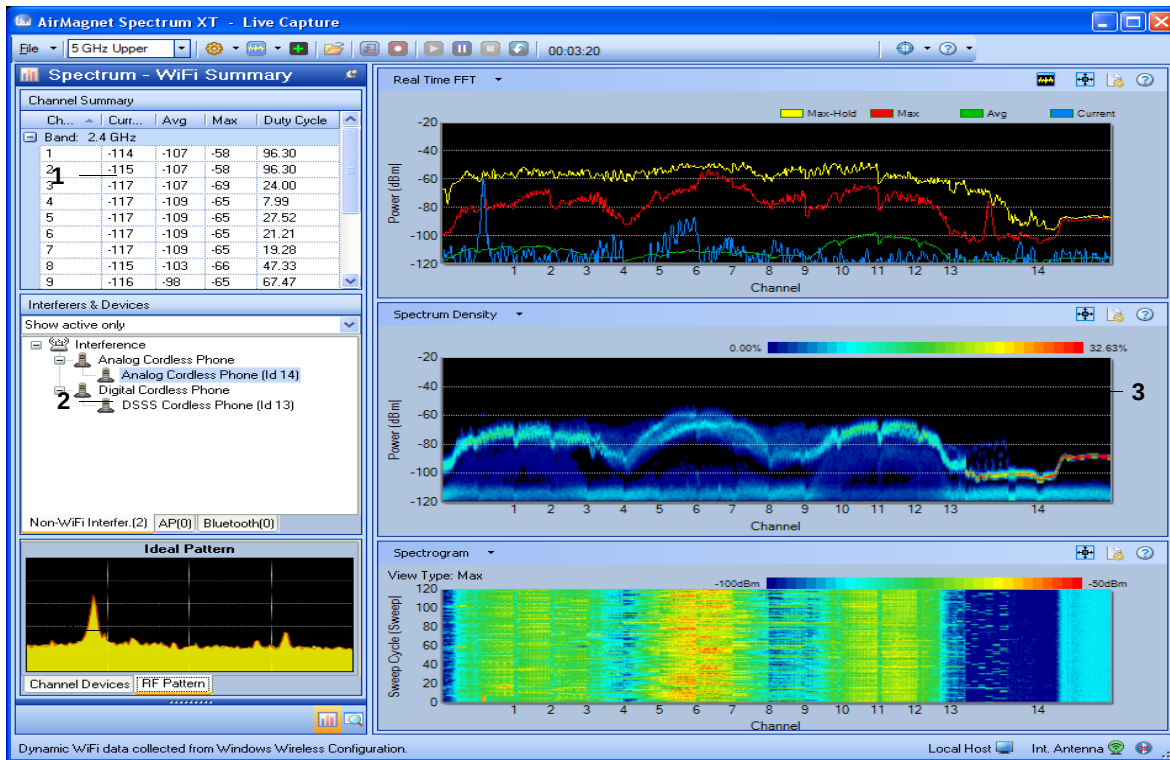


Figure 3-1: AirMagnet Spectrum XT Major UI Components

Table 3-1 provides the names of the UI components highlighted in Figure 3-1. Each of these components is discussed in detail in the rest of this chapter.

Table 3-1: AirMagnet Spectrum XT UI Components

ID	Screen Name
1	Toolbar
2	Spectrum-WiFi Summary
3	Graph Window
4	Channel Scan Indicator

Toolbar

The toolbar contains all the tools for operating AirMagnet Spectrum XT. While some of the tools have their names spelt out, others come with a tool tip which will reveal the name of a tool when you place the cursor over it. Many of them contain submenus in the form of a drop-down list menu, as indicated by the down arrow next to it. Figure 3-2 highlights all the tools on the toolbar. Detailed descriptions of these tools are presented in Table 3-2.

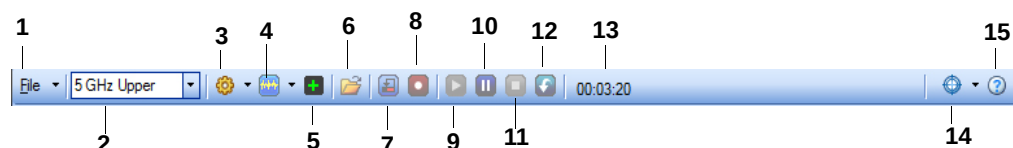


Figure 3-2: AirMagnet Spectrum XT Toolbar

Table 3-2: AirMagnet Spectrum XT Menus/Tools

ID	Tool Name	Description
1	File	Contains the following submenu: • Open Captured File... - Opens an AirMagnet Spectrum XT capture (.amt) file and starts the playback mode. • Save Capture As... - Save to a file the data being played or having been played. • Start/Resume - Starts or resumes live capture after it has been stopped or paused. • Pause - Pauses live data capture. • Stop - Stops file playback or data recording. • Instant Playback - Instantly starts playing back data captured in the last two minutes. • Record - Records captured data to the system's hard drive. • Live Capture - Switches to live capture mode from playback mode. • Remote XT Connection - Connect to a remote machine and view remote data. • List of Recent Files - Shows all recently opened capture files. • Exit - allows you to close the application.

Table 3-2: AirMagnet Spectrum XT Menus/Tools

ID	Tool Name	Description
2	Band	Contains the following options (which determine the 802.11 radio spectrum the application focuses on): • 2.4 GHz - covers the radio frequency range from 2.402 GHz to 2.842 GHz, which is used by Channels 1 through 14. • 5 GHz Lower - covers the radio frequency range from 5.17 GHz to 5.33 GHz, which is used by Channels 44, 48, 52, 56, 60, and 64. • 5 GHz Middle - covers the radio frequency range form 5.49 GHz to 5.71 GHz, which is used by Channels 108, 112, 116, 120,124, 128, 132, 136, and 140. • 5 GHz Upper -covers the radio frequency range from 5.735GHz to 5.835 GHz, which is used by Channels 157, 161, and 165. • 4.9 GHz - covers bands used by many public safety organizations, from 4.91 to 4.99 GHz. • Mixed - covers all aforementioned radio frequencies (other than 4.9 GHz) and channels.
3	Settings	Contains the following options: • Configure - opens the Configure dialog box which lets you configure the parameters in the application • SNMP Settings - sends SNMP traps to multiple SNMP management stations. • Custom Device Classification Manager - lets you identify, classify, and analyze interferers beyond those devices included in the software package. • Show Auto Detected Patterns - displays persistent patterns and enables you to create custom pattern signatures.
4	X-Axis Label Type	This button allows the user to modify the labels used on the X-axis for the graph displays. Users can specify viewing by band or by channel as desired. See “Modifying Display Options” on page 37 for more details.
5	Add View	Click this + button to add a new graph to the graphs view. Enables up to 9 graphs to be opened. Right-click on a view to display the close view option.
6	Open Capture File	Brings up the Open dialog box which enable you to open a capture (.amt) file.
7	Switch to Instant Playback	Starts playing back data captured in the last two minutes. <i>Note:</i> Once the playback is started, the button changes to Save Capture which enables you to save the data that has just been played back on the screen. The Start Recording button also changes to Switch to Live Capture which allows you to switch the application back to the Live Capture mode.
8	Start Recording	Enables the application to start recording captured data to the system's hard drive. <i>Note:</i> Once the recording starts, the button changes to Stop Recording and Save Capture, which allows you to stop and save the recorded data to an .amt file.

Table 3-2: AirMagnet Spectrum XT Menus/Tools

ID	Tool Name	Description
9	Resume/ Play	In live capture mode, this button is named Resume which allows you to resume live capture after it is paused. In playback mode, it is named Play which allows you to play back the data or file after the playback is stopped.
10	Pause	Pauses live data capture. <i>Note: Even though live data capture appears suspended on the user interface after you have clicked this button, the application is still capturing live data “behind the scene”. Clicking Resume/Play (after live capture is paused) will resume live capture mode with live data showing on the screen.</i>
11	Stop Live Capture	Stops live capture mode.
12	Reset Data	Resets all data in the application. <i>Note: The screen refreshes every time you click this button.</i>
13	Timer	Shows the progress of file playback. In Instant Playback mode, it shows the progress of the data playback.
14	Easy View	Provides certain combinations of graphs displayed in the graph window: • Spectrum View - displays Real Time FFT, Spectrum Density, and AP Signal Strength. • Density View - shows Spectrum Density, Channel by Speed, and Top 10 APs by Speed. • RF Usage View - shows Real Time FFT, Spectrogram, and Spectrum Density. • RF Channel View - shows Real Time FFT, Channel Duty Cycle, and Channel Power. • Device Occupancy View - shows Real Time FFT and Channel Occupancy. • WiFi Device View - shows WiFi devices only. • Non-WiFi Device View - shows non-WiFi devices only. • Add Current View... - allows you to name the current screen display and add it to Easy View. • Delete Custom View... - allows you to delete a custom view from Easy View. • Save Current View - allows you to save any custom view you have created and/or any configuration changes you have made in any graph currently shown in the graph window. • Saved Custom View - shows all custom view options the user has saved.

Table 3-2: AirMagnet Spectrum XT Menus/Tools

ID	Tool Name	Description
15	Help	Contains the following submenus: • Content - opens the Content tab of the online Help. • Search - opens the Search tab of the online Help. • About - open the About AirMagnet Spectrum XT dialog box which contains the following three tabs: • AirMagnet Spectrum XT - shows basic information about AirMagnet Spectrum XT. • License - shows your AirMagnet Spectrum XT license information. • Debug - provides an option for capturing sampling data needed for debugging.

Spectrum-WiFi Summary

Below the toolbar, on the right-hand side of AirMagnet Spectrum XT's user interface is the Spectrum-WiFi Summary. As its name suggests, this part of the screen provides an overall summary of spectrum and/or WiFi data that AirMagnet Spectrum XT has captured on your network. As shown in Figure 3-3, the Spectrum-WiFi Summary consists of three parts: Channel Summary, Device List, and Channel Devices/Device Pattern, each showing a specific type of data.

Channel Summary

The upper part of the Spectrum-WiFi Summary is Channel Summary. It summarizes the various energy readings captured on each of the channels in the selected radio band. See Figure 3-3.

Channel Summary					
	C	Cu...	Avg	Max	Duty Cycle
Band: 2.4GHz					
1	-80	-97	-58	32.40%	
2	-83	-97	-58	36.48%	
3	-88	-97	-55	39.02%	
4	-95	-99	-52	50.25%	
5	-100	-98	-49	12.90%	
6	-96	-97	-49	25.27%	
7	-96	-97	-49	63.27%	
8	-90	-94	-49	36.78%	

Figure 3-3: Channel Summary

The channels shown here vary, depending on the option you select from the Band menu on the toolbar. The data are from all sorts of devices that are operating on each of the channels. They include both WiFi devices and non-WiFi devices such as bluetooth devices, microwave ovens, and fluorescent lights that emit energy. You can see graphical presentations of the same data in the spectrum and WiFi graphs on the right-hand side of the screen. If you want to focus your attention on a particular channel in the graphs, simply select (click) the channel of your interest here. The selected channel will become highlighted in the graphs on the right.

Table 3-3 briefly describes the data displayed in this part of the screen.

Table 3-3: Channel Summary Data Description

Column	Description
Channel	All available channels in the selected radio band.
Current	The average of current FFT readings in dBm on each channel.
Avg	The average historical FFT readings in dBm on each channel.
Max	The maximum FFT reading in dBm on each channel.
Duty Cycle	The percentage of time the RF energy (both 802.11 and non-802.11) is present on the channel.

When the user selects a channel from the Channel Summary, that channel's portion of the wireless spectrum is highlighted in the charts displayed to the right. This makes it easy to identify exactly where a device is appearing in charts like the Spread Spectrogram, among others.

Device List

Below Channel Summary is the Device List. It shows all the Devices (WiFi and non-WiFi) that the application has detected in the network. The Device List contains two tabs that categorize devices based on their wireless characteristics; standard 802.11 Wi-Fi devices are displayed on their own tab, and non-802.11 devices on a second one.

When viewing the 802.11 devices portion, the drop-down menu across the top of the pane can be used to change the manner in which the devices are displayed, either by SSID or by Channel. See Figure 3-4.

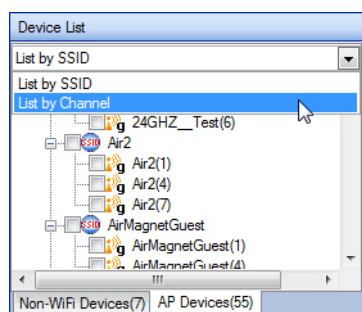


Figure 3-4: Choosing an AP List option

You can project signal strengths of any APs over the Spectrum Density graph by selecting them (checking the corresponding check boxes in the AP List). Signal strengths of the corresponding APs will appear in the graph in the form of color-coded curves.

Channel Devices

The bottom part of the Spectrum-WiFi Summary is Channel Devices, which lists the number of APs, stations, and/or VoFi phones that have been detected on channel in the selected 802.11 radio band. Similar to the AP List above, this part of the screen is devoted to the display of WiFi data only. You must have an AirMagnet-supported external wireless network adapter in order for AirMagnet Spectrum XT to capture and display such data. See Figure 3-5.

Channel	AP	Sta...	Ph...
1	10	0	0
2	1	0	0
4	3	0	0
6	25	0	0
7	6	0	0
9	3	0	0

Figure 3-5: WiFi devices listed by channel

The Channel Devices pane only displays channels on which WiFi devices are detected. If you notice certain channels missing from this section, it means that no WiFi devices have been detected on those channels. Also, the channels shown here vary depending on the option selected from the Band menu in the toolbar. Users can click the Device Pattern tab to view a sample image of the detected spectrum pattern of devices detected. See “[Device Pattern](#)” on page 108.

Graph Window

The right-hand side of the screen is the graph window, which can display up to three graphs vertically at the same time even though the user do have the option to display one or two graphs using the Settings drop-down list menu. By default, the graph window displays the Real Time FFT, Spectrum Density, and AP Signal Strength graphs, but the user can change the content of the window using options in the Easy View list menu on the toolbar or by using options in the Spectrum Graphs or WiFi Graphs. See Figures 3-6 and 3-7.

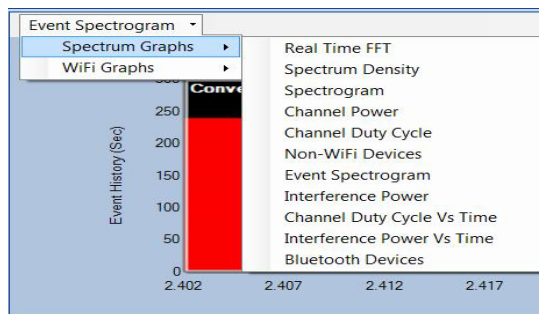


Figure 3-6: Spectrum graph options

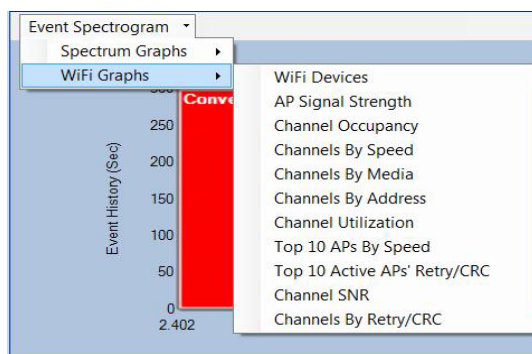


Figure 3-7: WiFi graph options

An AirMagnet-supported external wireless network adapter is required to view all options in WiFi Graphs. Otherwise, you will find some options showing limited static data while others simply being disabled.

In the upper-right corner of each graph is a  (Help) button. Clicking this button will bring up the AirMagnet Spectrum XT's online help page relevant to the graph. For all spectrum graphs, there is also a  (Chart Configuration) button that allow you to set or change certain parameters in the graph.

Channel Scan Indicator

The channel scan indicator which appears in the lower left-hand corner of the screen is available only when AirMagnet Spectrum XT is operated with a supported external wireless network adapter simultaneously with the spectrum adapter. It shows in real time the 802.11 channels that the wireless network adapter has been scanning. The channels that are scanned vary, depending on the 802.11 radio band in use.

If no external wireless network adapter is used, AirMagnet Spectrum XT will still gather limited amounts of WiFi data from Windows Wireless Configuration. This status will be indicated by a message in the bottom-left corner of the screen: "Dynamic WiFi data collected from Windows Wireless Configuration".

Chapter 4: Menus and Tools

Chapter Summary

This chapter discusses the menus and tools in AirMagnet Spectrum XT and ways to use them to configure and manage the various parameters in AirMagnet Spectrum XT to better serve your needs. It covers the following topics:

- Selecting a radio band
- Adding additional graph views
- Managing data capture
- Configure General settings
- Creating a custom view option
- Deleting a custom view option
- Saving the current view
- Copying and pasting a graph to another application
- Saving a graph as an image file

Selecting a Radio Band

AirMagnet Spectrum XT can scan all available 802.11 radio bands. Each band covers certain frequency range and channels. To enable the user to conduct more focused analysis of their spectrum and WiFi environment, the application provides five band option as described in Table 4-1.

Table 4-1: Radio Band, Frequency Range & Channel Coverage

Band	Frequency Range (in GHz)	Channel Coverage
2.4 GHz	2.402 ~ 2.494	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
5 GHz Lower	5.17 ~ 5.33	36, 40, 44, 48, 52, 56, 60, 64
5 GHz Middle	5.49 ~ 5.71	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
5 GHz Upper	5.735 ~ 5.835	149, 153, 157, 161, 165
4.9 GHz	4.91 ~ 4.99	184, 188, 192, 196
Mixed	All frequencies listed above (except 4.9 GHz)	All channels listed above (except 4.9 GHz)

The radio frequency ranges and channels covered by each radio band as mentioned in Table 4-1 apply to US and North America only. They may vary in other countries or regions of the world.

Switching from one radio band to another will cause the application to discard old data captured on the ‘old’ radio band before it starts scanning the “new” band. For this reason, changing bands is like resetting the application. The user should expect a sudden drop in the amount of data shown on the screen before they back up again.

By default, the application scans the 2.4 GHz radio band when it is started.

To change radio band:

- 1) From the toolbar, click the band menu.
- 2) From the Band drop-down list menu, select another band of interest. See [Figure 4-1](#).

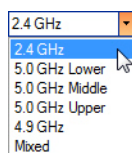


Figure 4-1: Band options

Add View

Click the + button on the toolbar to add an additional graph to the graphs view. This option enables up to 9 graphs to be opened. Right-click a graph to display the close view option. See [Figure 4-2](#).

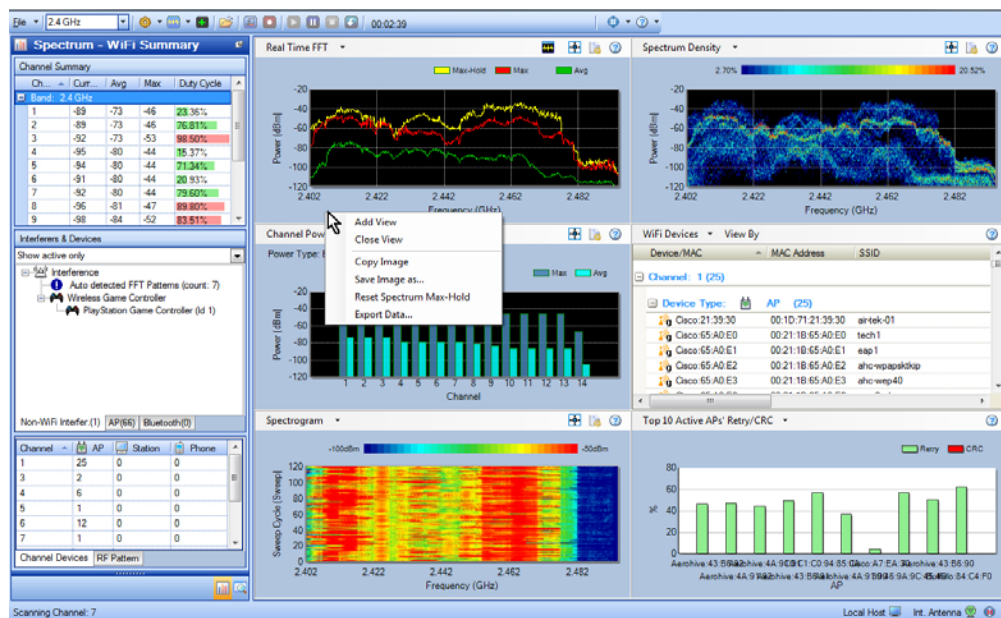


Figure 4-2: Add View showing right-click options

Managing Live Data Capture

By default, AirMagnet Spectrum XT is able to capture live spectrum and WiFi data and display them on the screen in real time. To enable the user to conduct focus analysis of any specific segment of data flow that has been captured, the application offers a number of tools on the toolbar that the user can use to suspend, resume, stop, and restart live capture as needed.

Pausing and Resuming Live Capture

Pausing live capture allows the user to suspend the dynamic display of live data on the screen; it does not stop the application from capturing live data at all. In other words, the application still keeps capturing live data and storing them in the memory after the user has clicked the **Pause Live Capture** button.

To suspend the display of live data capture on the screen:

- 1) From the toolbar, click (Pause Live Capture).

To resume the display of live data capture on the screen:

- 1) Click (Resume Live Capture).

Instantly Playing Back Captured Data

AirMagnet XT allows users to replay captured data that has recently been displayed on the screen so that they can revisit the data for a closer look.

To replay captured data that has just been displayed on the screen:

- 1) Click  (Switch to Instant Playback) on the toolbar. The application will start to play back the capture data that has just been displayed on the screen. See [Figure 4-3](#).



Figure 4-3: Instant playback of capture data

The application can instantly play back data captured in the last two minutes at most. The replay stops when the slider reaches the end. You can use the Play, Pause, Stop buttons to play the data back and forth. You can also set the starting point for the playback by dragging the slider to anywhere they want.

You can also save as a .amt file the data that has just been replayed by clicking  (Save Capture), or switch back to live capture mode by clicking  (Switch to Live Capture).

If you click **Save Capture**, the application will open the Save As dialog box so that you can save the data. However, the application stays in Instant Playback mode and automatically restart instant playback once the file is saved. You must click the Switch to Live Capture button in order to get out the Instant Playback mode.

Recording a Live Capture Data

Normally, the application automatically sends all data it has captured to the buffer. Due to the buffer size, the application discards old data as new data come in. However, if users want to retain data captured during a session, they can let the application to send the data to the system's hard drive. This is the so-called "stream to file" feature.

To use this feature, users must set the Max Live Capture Streaming File Size (MB) which is 500 MB by default. Users can set it to any value (up to 2 GB) so long as they have enough hard drive space to accommodate it. This can be done using **Configure>General> Max Live Capture Streaming File Size (MB)**.

To record capture data:

- 1) Click  (Start Recording).

The application will start record live capture data to the PC's hard drive. The recording automatically stops when the Max Live Capture Streaming File Size is reached. At that point, you will be prompted to save the file. You can either save the data to a .amt file or decline the prompt. However, all recorded data will be lost unless you save them. See the following section on how to save a recorded data to a file.

Saving Recorded Data to File

You will be prompted to save the data recorded to your PC's hard drive when the recording has reached the Max Live Capture Streaming File Size you have specified or when you interrupt the recording by clicking  (Stop Recording and Save Capture).

All recorded data are saved in a .amt file which can be played back in the application for further analysis. You must name the file and specify the location where the file is saved.

Opening a Capture Data File

Captured data are saved to a file using the .amt file extension. You can replay those saved capture data by opening the file containing the data.

To open a capture file:

- 1) Click  (Open Capture File).
- 2) Locate the .amt file on your PC and click Open.
- 3) Use the buttons (Start, Pause, and Stop) to play the file back and forth, if you wish to.
- 4) To switch back to Live Capture mode, click  (Switch to Live Capture).

Resetting Collected Data

Clicking the Reset Data button will cause the application to discard all spectrum and Wi-Fi data it has captured and then starts all over again.

To reset data:

- 1) From the toolbar, click  (Reset Data).

Configuring AirMagnet Spectrum XT Settings

AirMagnet Spectrum XT allows the user to fine-tune its system parameters so as to better serve its intended purposes. System configuration mainly involves the manipulation of WiFi and spectrum parameters in the application. It may also involve the selection of a WiFi driver when more than one WiFi driver is installed on the PC. Both these tasks can be performed in the Configure dialog box that will appear when you click **Settings>Configure...** from the toolbar.

Configuring WiFi and Spectrum Parameters

The configuration of AirMagnet Spectrum XT's WiFi and spectrum parameters affects the way WiFi and spectrum data are displayed on the screen. It allows the user to decide what data are to be displayed and how they are displayed.

To set or change the display of WiFi or spectrum data:

- 1) From the toolbar, click **Settings>Configure...** The default Configure dialog box appears.

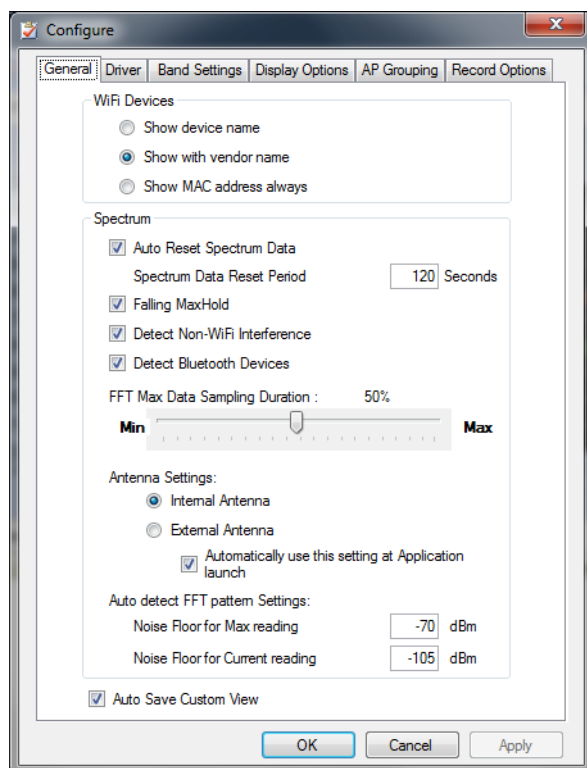


Figure 4-4: Configuring General settings

- 2) Make the selections as described in Table 4-3.
- 3) Click **Apply** and then **OK** when done.

Table 4-2: Configuring AirMagnet Spectrum XT's General Settings

Parameter	Description
WiFi Devices	These parameters apply to WiFi devices only.
Show device name	If selected, the names of WiFi devices will show on the screen wherever applicable.
Show with vendor name	If selected, vendor names will show as part of devices names on the screen.
Show MAC address always	If selected, MAC addresses will always appear as part of device identification.

Table 4-2: Configuring AirMagnet Spectrum XT's General Settings

Parameter	Description
Spectrum	This parameter applies to spectrum data only.
Auto reset spectrum data	If selected, AirMagnet Spectrum XT will automatically reset spectrum data at the interval specified by the user. See below.
Spectrum data reset period	(This option becomes available only when Auto reset spectrum data is selected. See above.) Specify the interval for the application to reset spectrum data.
Falling MaxHold	Factors such as noise in the spectrum or DC leak may cause sudden one-time spurts in the FFT plot. These spurts or "false" MaxHold, if left as is, will remain on the spectrum plot as MaxHold. This option, if select, enables the application to automatically discount the "false" MaxHold points by letting the "false" MaxHold gradually fall back, thus eliminating false MaxHold.
Detect Non-WiFi Interference	When Device Detection is disabled, Spectrum will not record devices detected durring scanning. This can reduce the number of entries that appear in the capture file, particularly when saved in .csv format.
Detect Bluetooth Devices	This option is used with a Bluetooth adapter to detect different Bluetooth devices in the area.
FFT Max Data Sampling Duration	The FFT Data Sampling feature can effectively reduce noise in order to produce a better distinguishable FFT pattern. For example, adjusting the bar to 50% will reduce sampling by half, thereby smoothing out spikes in the FFT graph that may be caused by interference noise.
Antenna Settings	This option allows the user to specify usage of the internal or external antennas with the AirMagnet Spectrum adapter. Check the Automatically use this setting at application launch option to store this setting for every time the application is loaded.
Auto Detect FFT Pattern Settings	The Auto Detect feature processes both the "current" and the "max" FFT data. As such these two parameters may be tuned in order to affect the algorithm. See "Auto Pattern Detection" on page 51.
Auto Save Custom View	If selected, the application will automatically save any custom view the user has created.

Selecting Another WiFi Driver

By default, each time you start AirMagnet Spectrum XT, the application will always look for and use the WiFi driver that was used in the previous session. If the user has only one WiFi driver installed on the PC, this should not be a problem. However, if you have more than one WiFi driver installed on the PC and you prefer to use a different WiFi driver than the one you used before, this may be somewhat inconvenient. This is where the Driver tab in the Configure dialog box comes into play. It allows you to select or switch to any WiFi driver of your choice.

To select another WiFi driver:

- 1) From the Configure dialog box, click the Driver tab. See [Figure 4-5](#).

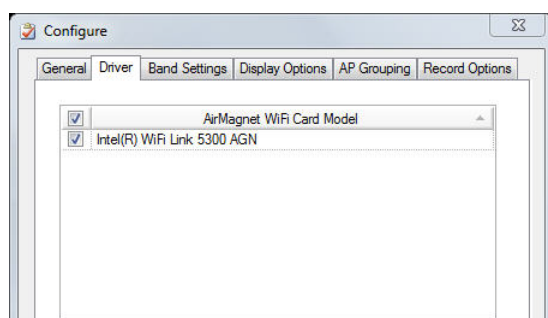


Figure 4-5: Selecting a WiFi driver

- 2) Select the desired driver.
- 3) Click **Apply** and then **OK**.

Specifying Band Settings

Users in regions with specific wireless range restrictions have the ability to specify precisely which channels shall be scanned in AirMagnet Spectrum XT by simply selecting the desired region from a drop-down provided in the application's configuration window. This streamlines the process of narrowing down the channels needed based on the area in which the network is located to a simple one-click process. Users may also select a frequency band from a provided list. See [Figure 4-6](#).

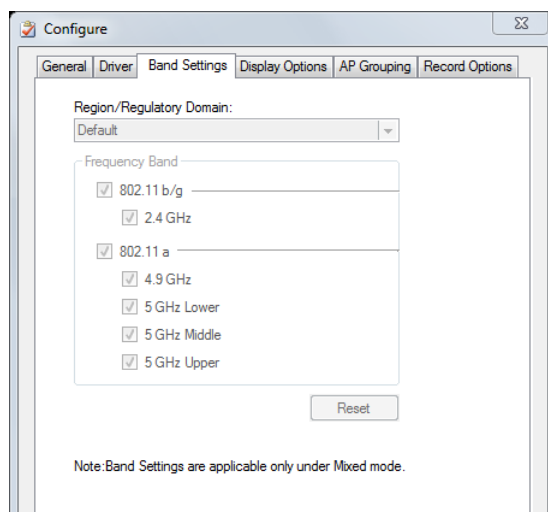


Figure 4-6: Band Settings Tab

Modifying Display Options

The Display Options tab allows the user to alter various aspects of the application's overall appearance. See [Figure 4-7](#).

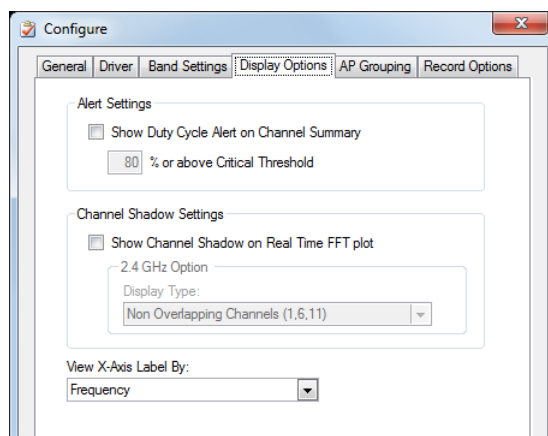


Figure 4-7: Display Options

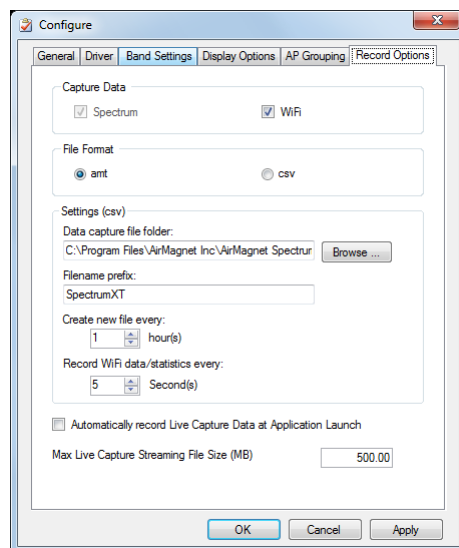
Refer to Table 4-3 for information regarding each of the options provided.

Table 4-3: Display Options

Option	Description
Alert Settings	When enabled, this option will highlight the Duty Cycle column in the Channel Summary field when it exceeds the specified threshold. Channels on which the Duty Cycle meets this criteria will be highlighted in red (channels with normal levels are highlighted in green).
Channel Shadow Settings	In WiFi deployment channels 1,6 and 11 in the 2.4 GHz spectrum are used. These settings highlight these channels to provide a better perspective of important channels.
Non Overlapping Channels	Shows non overlapping channels (1,6 and 11).
All Channels	Shows channels widths and locations of all the 802.11 channels in the band.
View X-Axis Label By	This allows the user to toggle between viewing charts by frequency range, channel number and by ZigBee Channel. Although the default setting is Frequency, many users may find the Channel selection easier to use and analyze.
Frequency	By default, users will view the data by frequency range (GHz).
Channel	Users may view the spectrum data at the central frequency of each channel.
Zigbee Channel	This specification is similar to Bluetooth with a shorter bandwidth. It is targeted at radio frequency applications that require a low data rate, long battery life, and secure networking.

Specifying Record Settings

By default, AirMagnet Spectrum XT saves collected data in AirMagnet's .amt format. However, the Record Options tab allows the user to save information in .csv format for analysis in other applications. The default format is .amt although .csv can also be selected to view the data in a spreadsheet format. The captured data can be viewed from both a Spectrum Analyzer adapter and a WiFi adapter.

**Figure 4-8: Record Options**

Files saved in .csv format cannot be played back using AirMagnet Spectrum XT.

To record .csv files:

- 1) From the Record Options tab, click the **csv** radio button.
- 2) Select either Spectrum data or Wifi data to be used.
- 3) Specify the folder in which the files should be saved, either by entering the path manually or by clicking the **Browse...** button.
- 4) Enter a prefix for the files, if desired.
- 5) Specify the frequency with which the files should be saved off.
- 6) Click **OK** to save the changes.

- **Automatically Record Live Capture Data at Application Launch:** This option allows the user to set a default to record live capture at launch of AirMagnet Spectrum XT.
- **Max Live Capture Streaming File Size (MB):** This option allows the user to adjust the maximum amount of data that will be captured in a single live capture instance (up to 2 GB).

Virtual AP Grouping

AirMagnet Spectrum XT's Virtual AP Grouping feature allows users to set up specific names for single devices that utilize multiple SSIDs under different BSSIDs. These groups help users identify instances where separate BSSIDs show up and appear to be several different devices, when they actually belong to a single device. See [Figure 4-9](#).

Spectrum comes with several built-in "automatic" AP Group rules. If you enable them, they will automatically group all devices meeting the criteria specified in the rule under a single AP Group.

To configure AP grouping settings:

- 1) From the Configure window, click the AP Grouping tab. See [Figure 4-9](#).

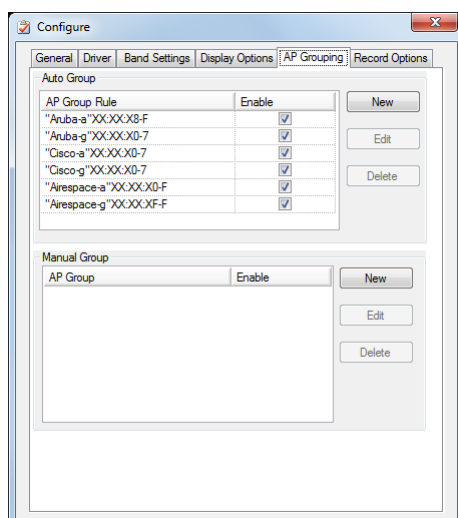


Figure 4-9: AP grouping tab

This tab provides two different types of rules for grouping APs. See the sections below for instructions on configuring each type.

Auto Group Rules

You may configure different fields in the Auto AP Group Rules by clicking on the New button. See [Figure 4-10](#).

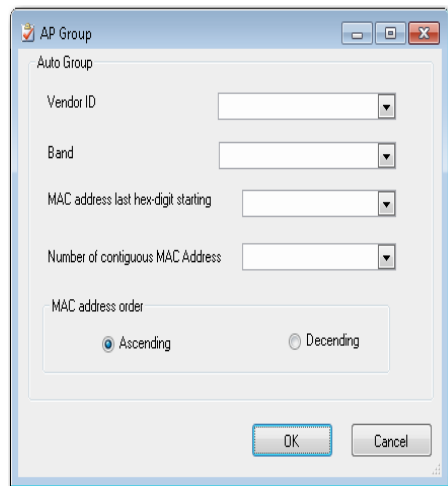


Figure 4-10: Editing an Auto Group

Manual Group Rules

You may manually add groups by clicking the New button for Manual Group and add a Group name and AP Name. See [Figure 4-11](#).

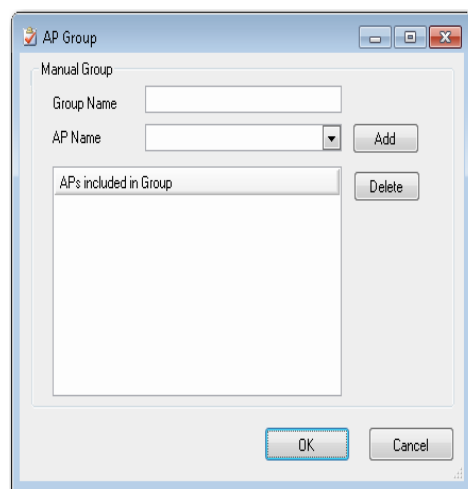


Figure 4-11: Adding a New Manual Group Remote Interface Access

With AirMagnet Spectrum XT 2.0.2, users have the ability to remotely log into the user interface and monitor ambient traffic patterns using a separate machine. In order to connect to the XT remote interface, users must install the AirMagnet Spectrum XT Viewer-Only license (provided with the purchase of a valid AirMagnet Spectrum XT license) on the second machine. From the secondary computer, users may simply launch the AirMagnet Spectrum XT application and use it to connect directly to the main licensed machine (using the machine's IP address). The spectrum data detected by the remote system will automatically populate the secondary computer's interface.

Integration of AirMagnet Spectrum XT with SNMP Management Stations

AirMagnet Spectrum XT provides a MIB file (AirMagnetSpectrumInterferer.mib) that allows AirMagnet Spectrum XT to send SNMP traps to multiple SNMP management stations when an interferer is detected by AirMagnet Spectrum XT. When you receive a trap from AirMagnet Spectrum XT, it is possible to view detailed description of the trap and thereby functioning of your wireless network. To receive traps from the AirMagnet Spectrum XT on your SNMP management station, follow these steps:

- From AirMagnet Spectrum XT, launch the SNMP settings dialog box by clicking Settings=>SNMP Settings menu. In the General tab, specify the IP addresses of all of your SNMP stations. The check box Send SNMP Traps should be enabled to send the SNMP traps. See [Figure 4-12](#).

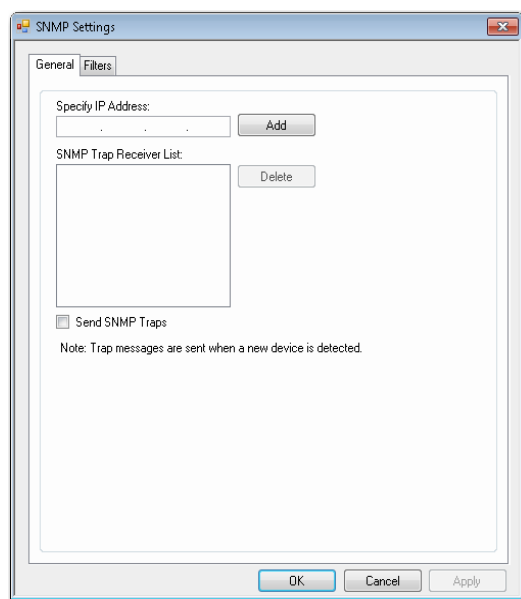


Figure 4-12: User can set various filters to control SNMP traps sent by AirMagnet Spectrum XT.

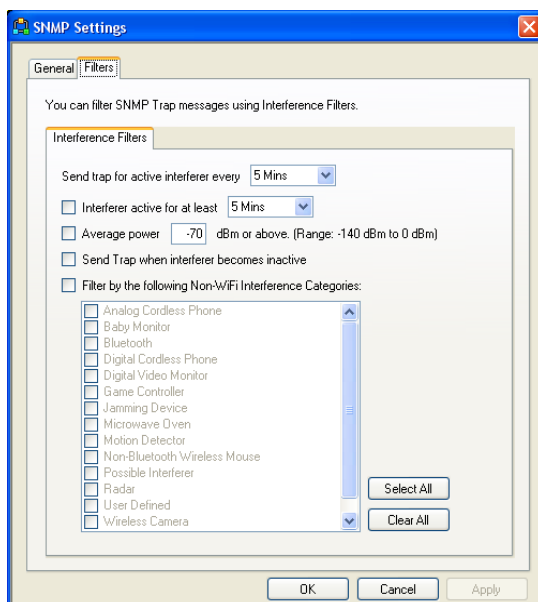


Figure 4-13: SNMP Filters tab

- Download AirMagnetSpectrumInterferer.mib from the download page of the AirMagnet Spectrum XT in your SNMP management station.
- Compile the MIB file and enable your SNMP management station to receive traps. Currently there is a trap that is generated by the AirMagnet Spectrum XT for each detected device based on the Filter conditions set in the Filter tab.
- The IANA assigned Private Enterprise Number for AirMagnet Inc. is 16603.

Integration of AirMagnet Spectrum XT with SNMP Management Stations

Table 4-4: Trap Details generated by AirMagnet Spectrum XT

Trap Number	SNMP Trap-V2	Related Alarm Title of Disct AirMagnet
1	amSpectrumTrap	Interferer detected

The trap will have the following details:

- Device Type
- Device Identifier
- Device Description
- First Seen Time
- Last Seen Time
- Channel
- Max Power at the Channel
- Average Power at the Channel
- Center Frequency of the Channel

Remote Spectrum Analysis

The **Remote Spectrum Analysis** feature can be used to give access to and control of the AirMagnet Spectrum XT application to a user that is offsite. This can be particularly useful for the IT professional needing to troubleshoot an issue at a remote location.

The Remote Spectrum Analysis interface is controlled through two menu options.

Connect to Remote Host - Opens a dialog where connection information about Remote Host IP Address, Port Number and (Security Password) Authentication key can be entered.

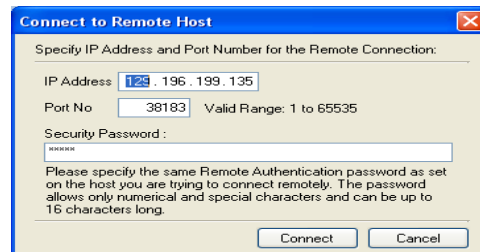


Figure 4-14: Remote Host Connection screen

Disconnect from Remote Host - This will disconnect the application from the remote Spectrum Analyzer mode. Live Capture will be stopped.

Before connecting to a remote machine, the user should have received an authentication key from the remote user. The Remote user should set the authentication key with the Remote Access Authentication menu which opens a dialog where the user can set the authentication key.

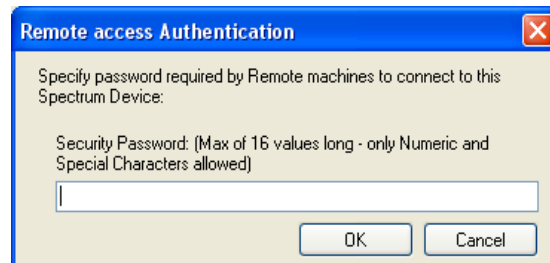


Figure 4-15: Remote Access Authentication screen

Using Easy View Options

The **Easy View** tool allows the user to filter data to be displayed on the screen so that they can focus more on data of interest. Figure 4-16 shows the default options in the Easy View drop-down list menu.

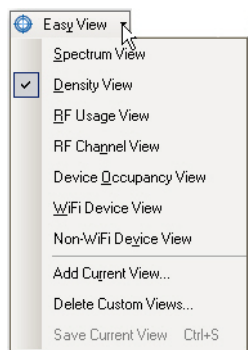


Figure 4-16: Easy View

The upper part contains the application's built-in easy view options; the lower part provides tools for creating, deleting, and saving custom view options. All custom view options that the user creates will be added to the bottom of the Easy View list menu.

Using a Default Easy View Option

AirMagnet Spectrum XT comes with a number of easy view options for the user to choose from. Table 4-4 briefly describes each of these options.

Table 4-5: AirMagnet Spectrum XT Default Easy View Options

View	Description
Spectrum View	(default) shows the Real-Time FFT graph, along with the Spectrum Density and AP Signal Strength graphs.
Density View	shows the Spectrum Density graph, along with Channels by Speed graph.
RF Usage View	shows the Real-Time FFT, Spectrogram and Spectrum Density graphs.
RF Channel View	shows the Real-Time FFT, Channel Duty Cycle, and Channel Power graphs.
Device Occupancy View	shows the Real-Time FFT and Channel Occupancy graphs.
Device View	displays the WiFi Devices table that list all WiFi devices (i.e., APs, stations, etc.) detected on each channel.
Add Current View	creates a unique view option using what is shown on the current screen and add it to the Easy View menu.
Delete Custom Views...	removes custom view options off the Easy View menu.
Save Current View...	saves the current view on the screen.
List of Custom Views	Lists all custom views that have been created.

By default, the application opens in Spectrum View, but you can switch to any other built-in option in the **Easy View** list menu.

To change to a different built-in Easy View option:

- 1) From Easy View list menu, click an option of your choice.

Creating a Custom View Option

Since the application can allow you to display a combination of three graphs on one screen, you can choose any three graphs of interest and save the current screen view as a custom view option. All custom view options are automatically added to the bottom of the Easy View list menu.

To create a custom view option:

- 1) Open three graphs of your choice on the screen.
- 2) From the toolbar, click **Easy View>Add Current View...** from the list menu. The New Easy View window appears. See [Figure 4-17](#).

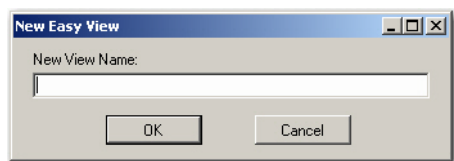


Figure 4-17: Creating a new Easy View

- 3) Type a name for the new view and click OK.

You can create more custom view options by following the same steps outlined above. All custom options you create will be automatically appended to the bottom of the Easy View list menu.

Deleting a Custom View Option

Unlike those built-in Easy View options, custom easy view options can be deleted if you want to.

To delete a custom Easy View option:

- 1) From the Easy View list menu, click **Delete Custom Views...** The Delete Easy Views window appears. See [Figure 4-18](#).

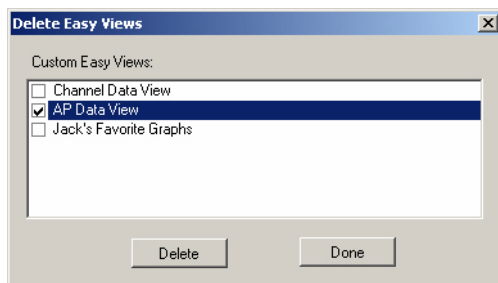


Figure 4-18: Deleting a custom view option

- 2) Select the custom view to be deleted.
- 3) Click **Delete** and then **Done**.

Saving Current View

Once you have created a current view, you can save it before closing the session. In this way, the next time you start the application, AirMagnet Spectrum XT will open in that same view that you have saved. You can either let the application do this automatically or do it manually by yourself.

Automatically Saving Current View

To let AirMagnet Spectrum XT automatically save the current view:

- 1) From the toolbar, click **Settings>Configure**.
- 2) Under the **General** tab, check **Auto Save Custom View**.
- 3) Click **Apply** and then **OK**.

*Once the **Auto Save Custom View** option is enabled, AirMagnet Spectrum XT will automatically save the custom view you have created before ending the current session and open in the same view at the next start.*

Manually Saving Current View

If you have not enabled the **Auto Save Custom View** option in the Configure dialog box (as discussed in the previous paragraph), you have to manually save the custom view that you have created before exiting the application by following the instructions outlined below. Otherwise, a message will pop up when you are trying to close the application, asking if you want to save the current view before exiting. It is then up to you to decide whether to save the current view or not.

To save the current view manually:

- 1) Open the graph or graphs of your choice.
- 2) From the toolbar, click **Easy View>Add Current View...**
- 3) From the New Easy View dialog box, name the current view and click **OK**.
- 4) With the current view you have just added shown on the screen, click **Easy View>Save Current View**.

Copying a Graph into Other Applications

AirMagnet Spectrum XT allows the user to easily copy any graph in the graph window as still images and paste them to other applications such as Paint, MS Word, etc. This makes it very convenient for saving and sharing data captured on the network.

To copy and paste a graph into another application:

- 1) Right-click a chart or graph of interest.
- 2) From the pop-up menu, select **Copy Image**. See [Figure 4-19](#).

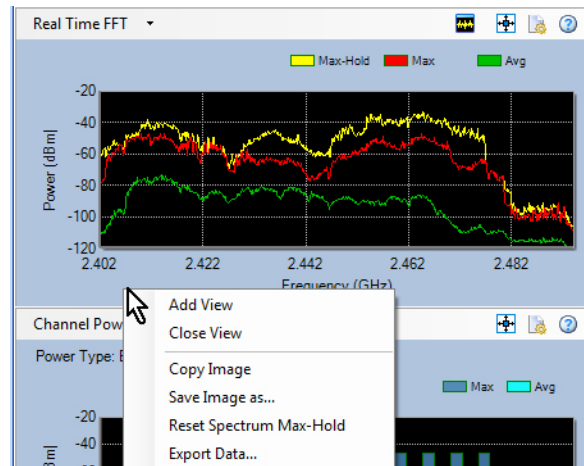


Figure 4-19: Copying a graph image

- 3) Open an application that supports copy and paste, such as MS Word.
- 4) Use the Paste command to paste the image to the document.
- 5) Save the document.

Saving Screen Data as Image Files

AirMagnet Spectrum XT allows the user to save any graph shown in the graph window as an image file in any of the following four image formats:

- .PNG
- .BMP
- .JPG
- .GIF

To save a chart or graph as an image file:

- 1) From the graph window, right-click the graph of interest.
- 2) From the pop-up menu, select **Save Image As . . .**. Refer to [Figure 4-19](#).
- 3) From the Save As dialog box, choose a location, name, and format for the file.
- 4) Click **Save**.

Dwell Time (FFT Max Data Sampling Duration)

This feature can effectively reduce noise in order to produce a better distinguishable FFT pattern. For example, adjusting the bar to 50% will reduce sampling by half, thereby smoothing out spikes in the FFT graph that may be caused by interference noise. To adjust the FFT Max Data Sampling Duration: :

- 1) From the toolbar, click **Configure> General Tab**.
- 2) Press and drag the bar between Min and Max.
- 3) Observe how it affects the Max (red) data line on the FFT Graph.

For more information about the FFT Graph, see Chapter 6: Analyzing Spectrum Data.

AirMagnet Spectrum XT Report

AirMagnet Spectrum XT Report will display a formatted report that summarizes RF spectrum data such as any detected non-WiFi interferers along with Wifi data such as detected APs (if a WiFi adapter is active). The report may be printed and exported.

Export options: .pdf, .rtf, .doc, .xls, and .rpt.

- 1) When installing AirMagnet Spectrum XT, accept the request to install the report viewer.
- 2) From the Navigation Bar, Click **Reports**.
- 3) Use the **page forward** and **page back** controls at the top of the report to navigate from page to page.
- 4) The report menu bar also provides options to **Print** and **Export**.

The first time the report is opened, it takes a snapshot of the data at that time. To update the data, click **Refresh**.

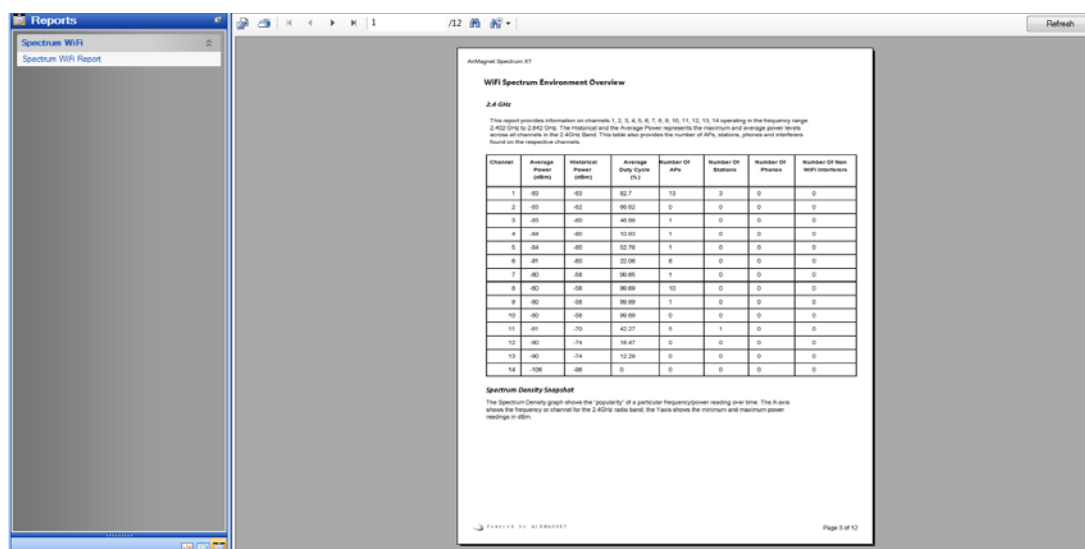


Figure 4-20: Report showing page 3 of 12

Chapter 5: Auto Pattern Detection and Custom Device Classification

Chapter Summary

This chapter discusses Auto Pattern Detection and Custom Device Classification, both features enabling users to identify, classify, and analyze interferers beyond those devices included in the software package.

- **Auto Pattern Detection:** The system identifies and lists persistent RF patterns that do not match its database of interferers. The user may name and save the pattern in order to have it show up as a named interferer in the future when that pattern is detected.
- **Custom Device Classification:** The user may create a custom signature of an RF pattern in order to have it show up as a named interferer in the future when that pattern is detected.

Auto Pattern Detection

During the course of an AirMagnet Spectrum XT session, if a particular RF pattern is persistently detected, a list item is created in the “Interferers & Devices” area named “Auto detect FFT Patterns.” This list item will show a sum count of the number of patterns detected. The count may rise and fall depending on whether a detected pattern continues to be persistent. See [Figure 5-1](#).

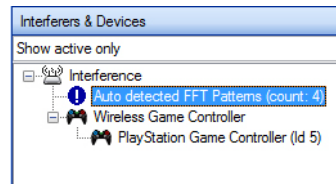


Figure 5-1: Auto detected FFT pattern

This feature is somewhat different from the Custom Device Classification Manager in that these patterns are defined by the system whereas you may manually define the pattern in the Custom Device Classification Manager.

You may view the pattern(s) and create custom signatures of any patterns using the “Auto detect – FFT Patterns” window.

Note: If a pattern is no longer detected after one minute, it will be removed from the Detected Patterns list and the pattern count will be reduced by one to reflect that the pattern is no longer detected.

This window may be opened by two methods:

- Double-click the “Auto detected FFT Patterns” line item under “Interferers & Devices”
- From the Gear drop-down, select “Show Auto Detected Patterns”

With this window open, you will see the list of detected patterns on the left. The highlighted pattern will be displayed in the FFT graph on the right (zoomed-in is the default). The pattern will either be “Max” or “Current” data depending on how the pattern was originally detected. The color coded legend in the upper right of the graph will indicate whether the data is “Max” or “Current.”

The legend above the patterns indicates that if a custom signature was previously created for a particular pattern, it will be highlighted in blue (as shown in the bottom pattern in [Figure 5-2](#)).

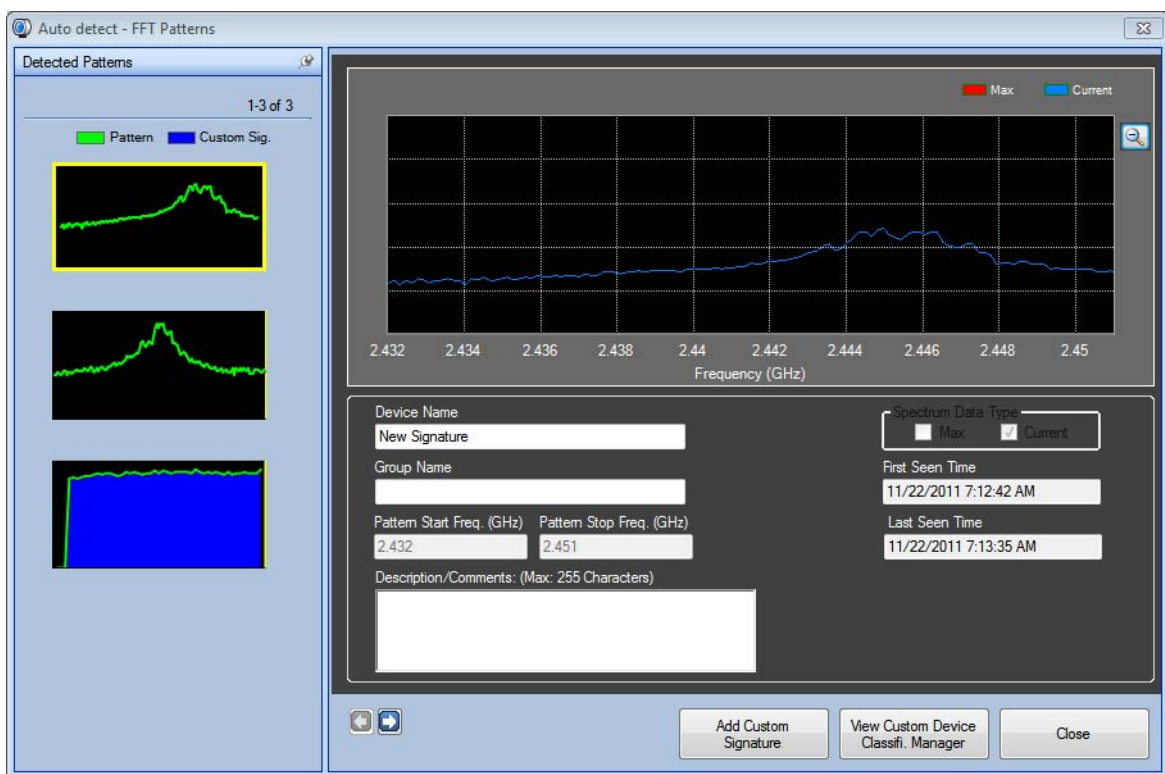


Figure 5-2: Auto Detect FFT Patterns window

To create a custom signature of a pattern:

- 1) From the **Settings** drop-down menu, select **Show Auto Detected Patterns**.
- 2) Click the desired pattern from the pattern list on the left side of the window.
- 3) Replace **New Signature** with a custom name for the signature.
- 4) You may also assign the signature to a group using **Group Name**. All signatures assigned to the same group will show up as children of that group in the Device Signature List that is part of the Custom Device Classification Manager.

Note: Both Pattern Start and Stop fields will be auto-filled with the frequency range.

- 5) Add any description comments, if desired.
- 6) Click **Add Custom Signature** to save the signature.

Once a signature is created it may be viewed and edited using the **Device Classification Manager**.

Note: Custom signatures may be imported and exported using the Custom Device Classification Manager.

Best Practices

How Auto-Detect Works:

The Auto Detect FFT Pattern feature in Spectrum XT looks for repeating patterns in the incoming FFT data. It does this by performing the following steps:

- 1) Performs a 7 point weighted average of the signal, to smooth out small changes in the FFT data.
- 2) Looks for points in the line that exit/enter the noise floor, producing FFT shape start/stop points.
- 3) These FFT shape start/stop points are categorized based on their start/stop frequency. They are compared against patterns seen in previous iterations of the algorithm. When the mean delta between patterns with the same start/stop frequencies is less than 5 dB, the pattern is said to have been observed again.
- 4) When the observation count for a particular pattern reaches 6, the pattern is said to have been Auto Detected and is now available for inspection in the UI.
- 5) Patterns which are not seen again within a 1 minute duration are recycled (thrown away). Thus, the user may observe the Auto Detected FFT Pattern count increase and decrease over time.

What the user can tune:

The Auto Detect feature processes both the “current” and the “max” FFT data. As such there are two parameters the user may tune in order to affect the algorithm: “Noise Floor for max Reading” and “Noise Floor for Current Reading”. See [Figure 5-3](#).

In RF environments where the FFT readings are consistently higher (or lower) than these values, the efficacy of the algorithm may be improved by tuning these values to match the lowest expected FFT readings for current and max respectively.

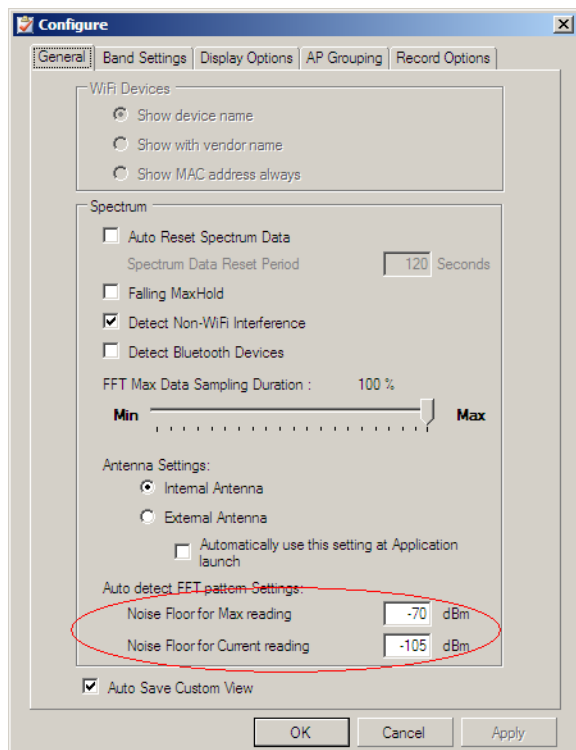


Figure 5-3: Auto Detect configuration

Custom Device Classification Manager

The first step in using custom classification is determining whether there may be an unclassified device detected in your environment. Each RF interferer has its own signature pattern on the Real Time FFT chart. This helps the user to recognize a distinct pattern for the device.

In [Figure 5-4](#), a pattern shows up that looks like a narrowband transmitter. At this point, if the device is not known to the user, a directional antenna would work best to locate the device within the environment for labeling in the custom classification.



Figure 5-4: Device Detected

To create a custom device classification signature:

- 1) First, wait until you see a distinct pattern for the device on the Max or Current Line of the FFT graph. By default, the visibility of Current Line is not enabled on the Real Time FFT chart. The user can enable it from the chart configuration window.
- 2) Click the **Add Custom Device Classification** button (this is located at the top left of the FFT graph, see Figure 5-4).
- 3) The slider bar on top of the Custom Device Window can be used to move forward or backward on the frames to capture a perfect pattern. This slider is in sync with the Instant Playback data with a maximum of 2 minutes worth of data. The slider bar is enabled only for the signature which is currently being defined. To get the most accuracy out of the custom signature feature, the user should select only the portion of the band which contains the interferer's distinct pattern. See Figure 5-5.

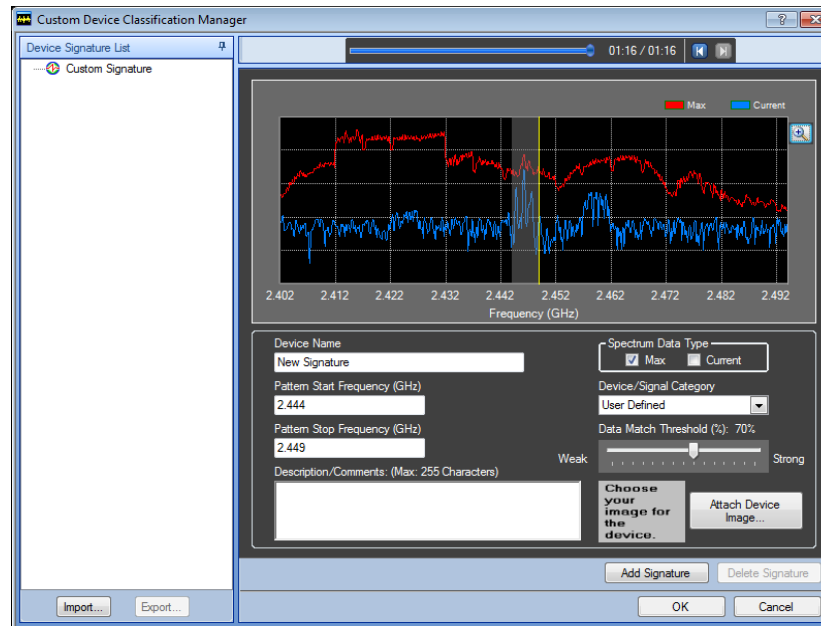


Figure 5-5: Range Defined Custom Classification Window

- 4) Narrow down the pattern window from the entire spectrum to just the frequencies that are relevant to the device. To do this, click the left edge of the desired range and drag to the right edge of the range.
- 5) Replace **New Signature** with a custom name for the signature.
- 6) You may also assign the signature to a group using **Group Name**. All signatures assigned to the same group will show up as children of that group in the Device Signature List that is part of the Custom Device Classification Manager.

Note: Both Pattern Start and Stop fields will be auto-filled with the frequency range.

- 7) Select whether to use the **Current** or **Max** data line for the **Spectrum Data Type**. This may depend on which is best based on which one provides a consistent, distinct pattern. Both data sources may be selected in order to have the system detect the defined pattern on either of the data sources. For example, hopping or short-burst devices should use the max setting for the Spectrum Data Type instead of the current, as the Max data gives a more distinct pattern in this situation.
- 8) The **Category** drop-down enables you to choose a pre-defined category to assign to the new signature.
- 9) The **Data Match Threshold** is used to define how loosely or tightly defined the signal pattern is. The Data Match Threshold value is 70%, and the user can change this to any

value between 30% and 100%. For environments with high amounts of spectrum data, most loosely constrained patterns can yield better detection rates, and can also lead to potential false detections. More tightly constrained patterns, meaning a higher threshold, means that there will be fewer false detections, with a chance that there will also be fewer actual detections that fall just out of range of the constraints.

- 10) Add any description comments, if desired.
- 11) Should you desire to attach an image to the new signature that may be used to easily identify the signature, click **Attach Device Image** to browse to an image .
- 12) Click **Add Signature** to save the signature.

The system allows to create a maximum of 50 custom signatures and at the most 10 signatures can be enabled. For an enhanced system performance, it is best to enable only the signatures which are of current interest to the user. See [Figure 5-6](#).

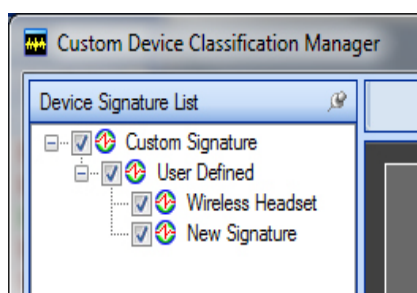


Figure 5-6: Enable and Disable Custom DeviceSignatures

Verification

The created custom signature is tightly coupled with the associated frequency of the pattern. If the device switches the channel and needs to classify on the new channel, the user must create signatures for those frequencies. Once the custom device has been defined and saved, the next time the correct conditions are met, the device will appear in the Device List and in the Non-WiFi devices panel. See [Figure 5-7](#).

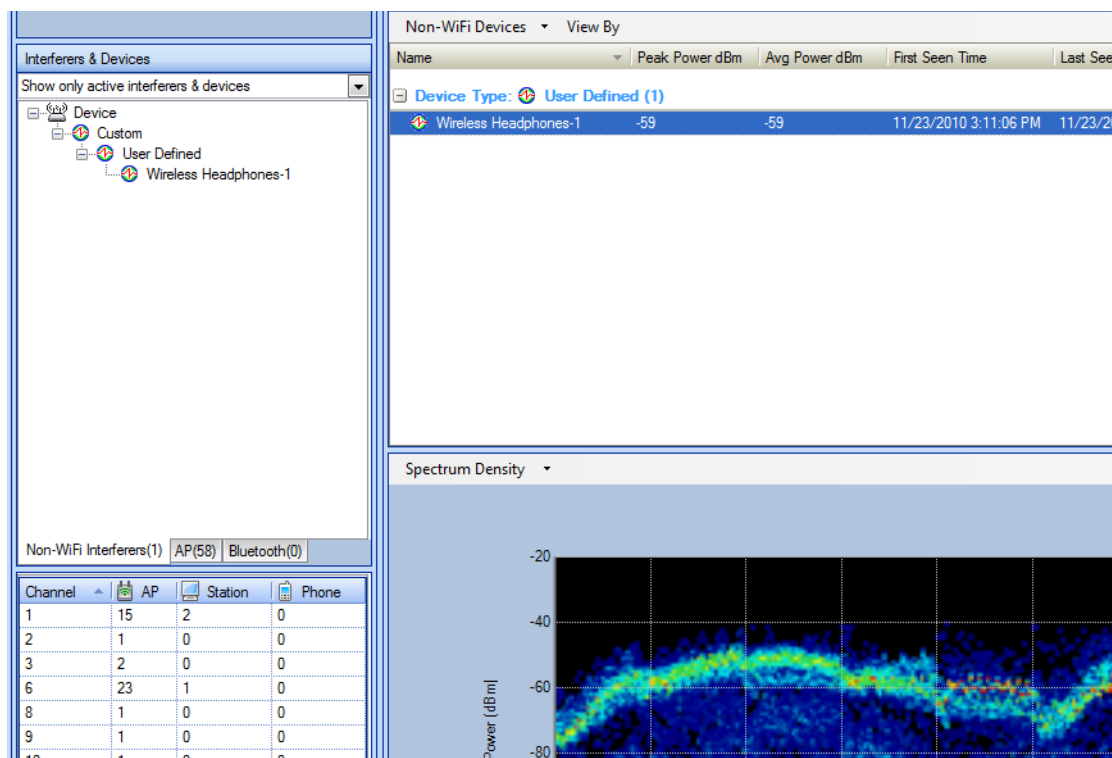
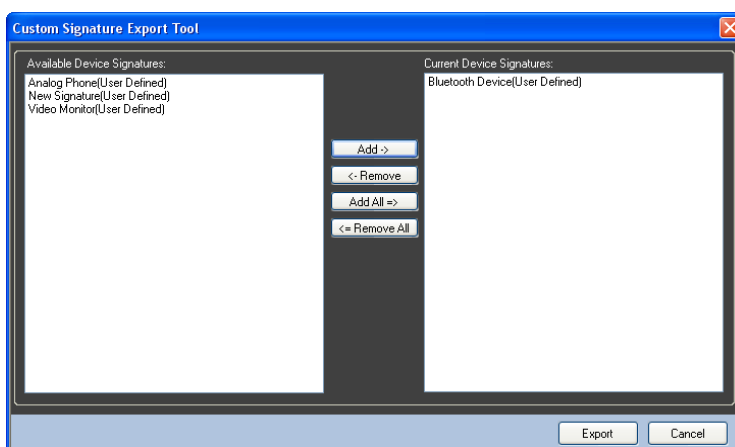


Figure 5-7: Device List and non-WiFi Devices Panel

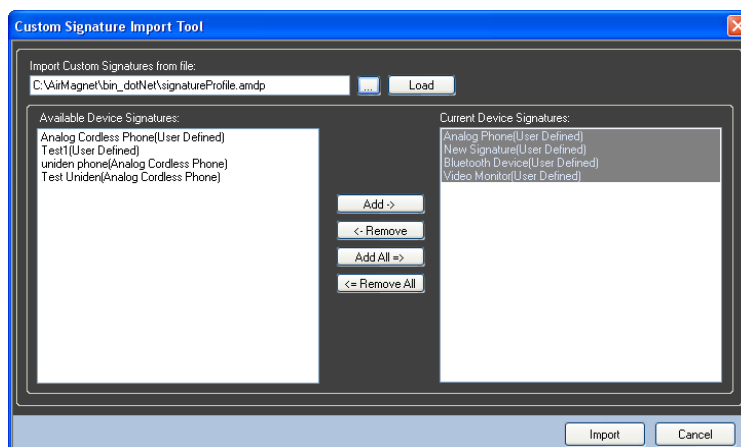
Export/Import Custom Signatures

AirMagnet Spectrum XT supports the ability to share the defined signatures between users. The user can export the interested signatures to a file which can be shared with other users. The user who received a signature file should import the signature into their system to make use of it.

The custom device classification window has buttons to export and import the custom signatures. The system has the ability to selectively export one or more signatures. The exported signatures will be saved into a file (.amdp) which users can share with other users. See [Figure 5-8](#).

**Figure 5-8: Signature Export**

The exported signatures from the file can be imported into the system by clicking the Import button and selecting the appropriate file. The available device signatures list all the signatures available on the file. The user can selectively import one or more signatures into the system. The imported signatures will be merged into the signature file persistent on the system. By default, the imported signature is not enabled and the user must enable them by clicking the check box on the Device Signature List. See Figure 5-8.

**Figure 5-9: Signature Import**

Custom Signature During File Playback

The custom devices classified during recording phase will not be saved into the trace file. Custom signatures will be reevaluated during file playback for possible classification of the custom devices. AirMagnet Spectrum XT does allow the user to create new custom signature in playback mode. Signatures defined during playback will be evaluated against the captured data for the device detection. The creation and application of custom signature during file playback is no different from the Live Capture.

Chapter 6: Analyzing Spectrum Data

Chapter Summary

This chapter discusses in detail the various spectrum graphs that AirMagnet Spectrum XT offers. It describes the data contained in each of these graphs and the ways to configure those graphs to customize the presentation and analysis of spectrum data captured on your network. It covers the following topics:

- Spectrum graph options
- Real Time FFT graph
- Configuring Real-Time FFT graph settings
- Spectrum Density graph
- Configuring Spectrum Density graph settings
- Spectrogram graph
- Configuring Spectrogram graph settings
- Channel Power graph
- Configuring Channel Power graph settings
- Channel Duty Cycle graph
- Configuring Channel Duty Cycle graph settings
- Non-WiFi Devices
- Event Spectrogram
- Configuring Event Spectrogram

Spectrum Graph Options

AirMagnet Spectrum XT has the capability to capture all sorts of spectrum data emitted from various non-WiFi devices on your wireless network and display in the following five spectrum graphs:

- Real Time FFT
- Spectrum Density
- Spectrogram
- Channel Power
- Channel Duty Cycle
- Non-WiFi Devices
- Event Spectrogram
- Interference Power

- Channel Duty Cycle vs Time
- Interference Power vs Time

All these graphs are listed in the Spectrum Graphs list menu, which is available in all individual graphs.

To access the Spectrum Graphs list menu:

- 1) From graph window, click the title of a graph.
- 2) From the drop-down menu, select Spectrum Graphs. See [Figure 6-1](#).

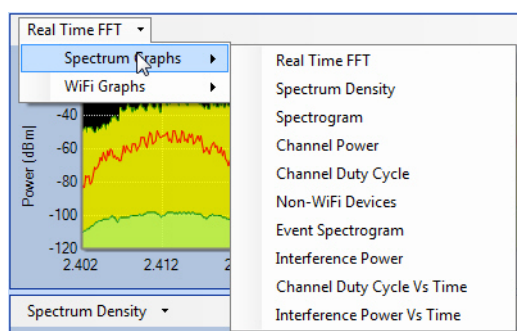


Figure 6-1: Spectrum Graph options

Real Time FFT

The Real-Time FFT (Fast Fourier Transform) graph displays in real time the value of RF power as a function of radio frequency. The X-axis shows the frequency range of each channel in the selected radio band; the Y-axis shows power readings in dBm. See [Figure 6-2](#).



Figure 6-2: Real Time FFT graph

As seen from [Table 6-1](#), the Real Time FFT graph may display four types of spectrum data that are color-coded. The number of data types displayed depends on the configuration settings.

Table 6-1: Real Time FFT Graph Parameters

Color	Spectrum Data	Description
Yellow	Max-hold	The highest power readings that have been recorded since the session began.
Red	Max	The maximum power in the RF Spectrum of a single channel sweep. Each FFT consists of 256 samples in 6.4 microseconds. A 100ms dwell on a channel results in 15,625 FFTs.
Green	Average	The average historical power readings recorded since the beginning of the session.
Blue	Current	The last sampling power in the RF Spectrum of a single channel sweep. <i>Note: The Current option is disabled by default; it can be enabled by modifying the Graph Options.</i>

You can see a brief text description of the spectrum data such as the Maximum, Average, and Current power readings as well as the radio frequency using the tool tip which, if enabled, will pop up where you place the causer in graph. See [Figure 6-3](#).

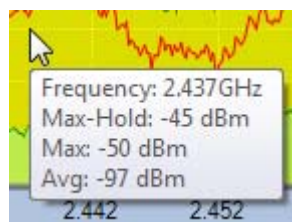


Figure 6-3: Using tool tip

The tool tip shows the following information about the point of interest in the Real-Time FFT graph:

- (RF) Frequency
- Max-hold (power reading)
- Maximum (power reading)
- Average (power reading)
- Current (power reading - if enabled)

Technically the power range in the Real Time FFT graph can be set as low as -140 dBm (Minimum Power) and/or as high as 0 dBm (Peak Power). When a narrower power range is used, e.g., -120 dBm ~ -30 dBm, the user may notice some discrepancy between what is shown in the Real Time FFT graph and what is displayed in the tool tip when the actual power readings fall beyond either or both the Minimum Power and/or Peak Power limit. For instance, if the power range is set between -120 dBm and -20 dBm, you will not be able to see any power reading lower than -120 in the graph because it falls beyond the Minimum Power. However, you will be able to see the actual power readings in the tool tip even when they fall outside the specified power range because the tool tip is not affected by the power range set for the Real Time FFT graph.

Note that the power readings shown in the tool tip are not updated in real time and may not match what is shown in the Real Time FFT graph.

Channel Duty Cycle Overlay on FFT Graph

The FFT Graph may be configured to show an overlay of Channel Duty Cycle data. This setting option is added to the FFT Chart Configuration settings as “Show Duty Cycle.”

With this option enabled, the duty cycle data will overlay the FFT graph as semi-transparent bars. Both WiFi and non-WiFi data are displayed as indicated by the legend in the upper right of the graph. The Duty Cycle percentage is shown on the far right Y-axis.

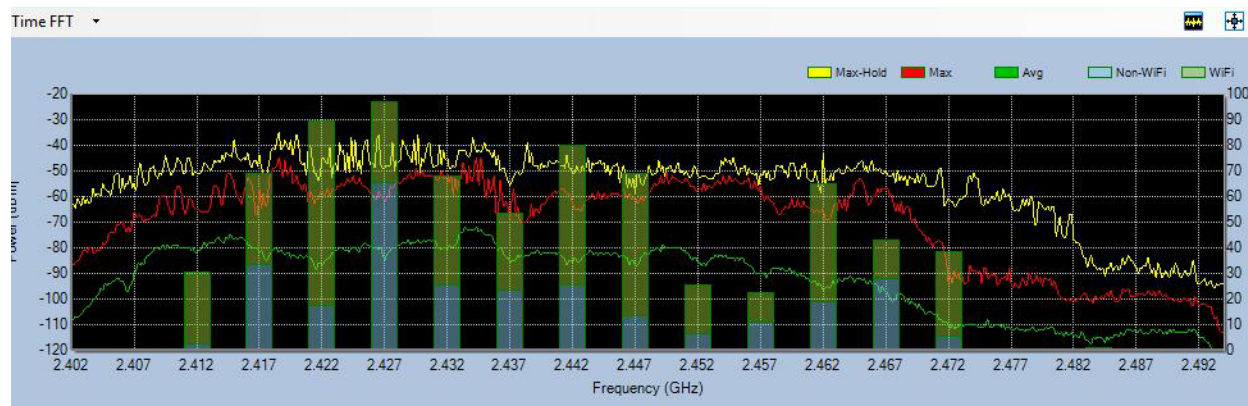


Figure 6-4: FFT Graph Showing Channel Duty Cycle

Setting FFT Graph Parameters

In the upper-right corner of the Real Time FFT graph comes with a Configuration button which allows you to set or change a number of parameters in the Real Time FFT graph.

To configure Real-Time FFT graph parameters:

- 1) From the upper-right corner of the Real Time FFT graph, click  (Chart Configuration). The Real-Time FFT Configuration dialog box. See Figure 6-5.

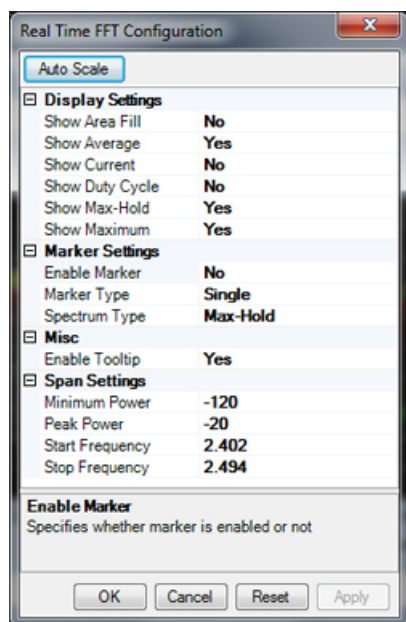


Figure 6-5: Configuring Real Time FFT graph

- 2) Make the entries and/or selections as described in the Table 6-2.
- 3) Click **Apply** and then **OK**.

Table 6-2: Setting Real Time FFT Graph Parameters

Parameter	Description
Show Area Fill	Enables or disables the graph's ability to fill the area below the displayed line. Note: This option can be fairly CPU-intensive; consequently, users may experience improved application performance if this is set to No.
Show Average	Allows the user to show or hide the average power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - displays the average power readings. • No - hides the average power readings.

Table 6-2: Setting Real Time FFT Graph Parameters

Parameter	Description
Show Current	Allows the user to show or hide the current power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - displays the current power readings. • No - hides the current power readings.
Show Duty Cycle	The duty cycle data will overlay the FFT graph as semi-transparent bars • Yes - displays the duty cycle overlay. • No - hides the duty cycle overlay.
Show Max-hold	Allows the user to show or hide the max-hold power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - displays the max-hold power readings. • No - hides the max-hold power readings.
Show Maximum	Allows the user to show or hide the maximum power readings in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - displays the maximum power readings. • No - hides the maximum power readings.
Enable Marker	Allows the user to enable or disable the marker or markers (which is or are tiny blue dots) on the FFT graph. The marker or markers help you to highlight a specific point of interest in the FFT graph. Click in the field and use the down arrow to select either of the following: • Yes - displays the marker. If selected, You then have to specify a marker type which can be Single or Delta. See below. • No - hides the marker.
Marker Type	Used only when you select True in the Enable Marker field. It allows you to choose between Single and Delta. The former only shows one marker, as the name suggests. The latter shows two markers: one of them stays at a fixed location on the FFT graph while the other can be dragged around. To effectively use this feature, you should start with a Single marker and drag it to a point of interest on the FFT graph. Then select Delta to bring up the second marker. This will cause the first marker to remain fixed at where you leave it. You can then drag the second marker to compare the power readings between a fixed data point and any other data point on the FFT graph. Click in the field and use the down arrow to select either of the following: • Single - displays a single maker which can dragged to any point of interest on the FFT graph. • Delta - displays two markers: one fixed at a particular location and the other can be dragged across the FFT plot for comparison. See the above paragraph. Note: When Marker is enabled, power readings of the data points marked by the markers also appear in the upper-left corner of the FFT graph.

Table 6-2: Setting Real Time FFT Graph Parameters

Parameter	Description
Spectrum Type	Allows the user to decide where (which part of the FFT graph) the marker or markers should fall. Click in the field and use the down arrow to select one of the following: • Current - places the marker or markers on the Current power readings. (The marker may jumps up and down as the curve line changes, because this curve reflects the real-time change of power readings across the spectrum.) • Average - places the marker or markers on the Average power readings. • Maximum - places the marker or markers on the Maximum power readings.
Enable Tool Tip	Allows the user to show or hide the tool tip (on the FFT graph), which provides the current, average, and maximum power readings as well as the frequency at the point the cursor rests upon. Click in the field and use the down arrow to select either of the following: • Yes - shows the tool tip. • No - hides the tool tip.
Minimum Power	Allows the user to set or change the minimum power level on the Y-axis. By default, it is set at -120 dBm, but it can be set to as low as -140 dBm. Highlight the existing value and override it with a new value.
Peak Power	Allows the user to set or change the maximum power level on the Y-axis. By default, it is set at -20 dBm, but you can change it to any value less than 0 dBm. Highlight the existing value and override it with a new value.
Start Frequency	Allows the user to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	Allows the user to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

The text message at the bottom of the Real Time FFT Configuration dialog box changes with the parameter you select. It provides a brief description of the parameter being selected.

Spectrum Density Graph

The Spectrum Density graph shows the “popularity” of a particular frequency/ power reading over time. The X-axis shows the frequency or channel for the selected 802.11 radio band; the Y-axis shows the minimum and maximum power readings in dBm. See [Figure 6-6](#).

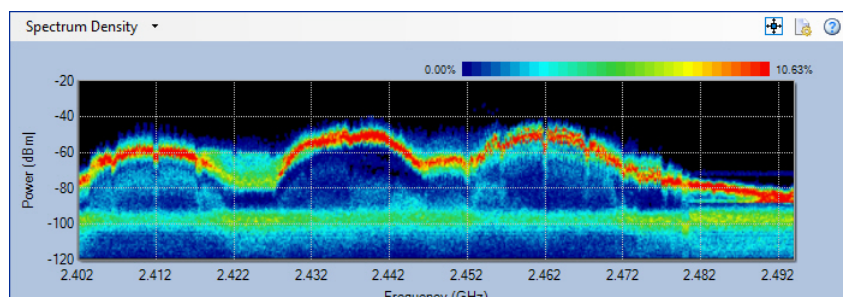


Figure 6-6: Spectrum Density graph

Viewing AP Signal Strengths Across Frequency Range

You can also display the signal strengths of APs selected from the AP List by SSID/Channel on the left-hand side of the screen. The signal strengths of the selected APs appear in the form of curves across the corresponding frequency range used by the APs. Notice that the selected APs and their signal strength readings are color-coded with matching colors for easy identification. See Figure 6-7.

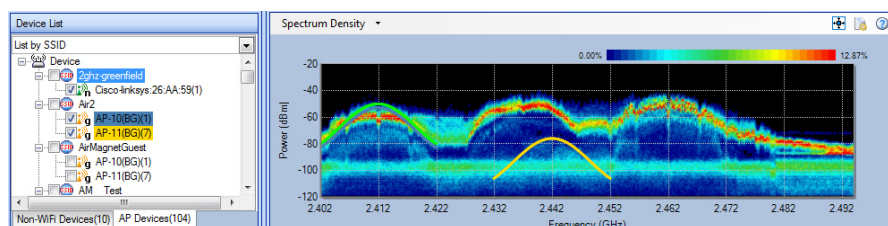


Figure 6-7: Showing AP signal strength in Spectrum Density graph

The AP signal strength curves are based on WiFi data captured by the wireless network adapter in use and may not completely match the spectrum plot. As shown in Figure 6-7, AP signal strengths as represented by the colored curves appear higher than the maximum signal strength shown in the Spectrum Density graph. This is because AP signal strengths (and the curve representing them) are based on RSSI data captured by the external wireless network adapter. While RSSI is usually calculated over a packet or averaged over multiple packets, RF power as measured by the spectrum analysis engine includes packets and background noise, plus RF silence in between the packets. For this reason, it is no surprise that the RSSI value (the AP curve in this case) differs from the peak of the spectrum graph for the same AP.

Configuring Spectrum Density Plot Parameters

You can set or change the settings of the Spectrum Density graph the same way as you do with the Real Time FFT graph.

To configure Spectrum Density graph parameters:

- 1) From the upper-right corner of the Spectrum Density graph, click  (Chart Configuration). The Spectrum Density Configuration dialog box. See Figure 6-8.

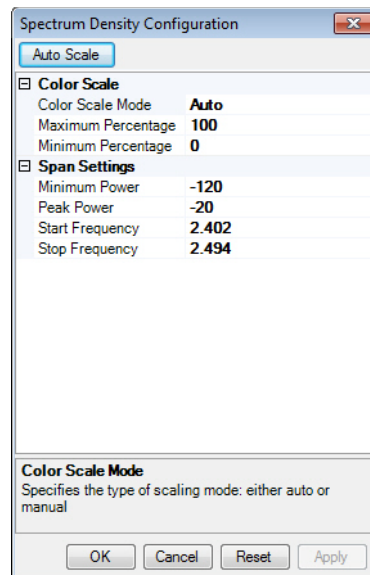


Figure 6-8: Configuring Spectrum Density graph

- 2) Make the desired selections and/or entries as described in Table 6-3.
- 3) Click Apply and then OK.

Table 6-3: Setting Spectrum Density Graph Parameters

Parameter	Description
Color Scale Mode	Allows the user to set or change the color scale modes of the Spectrum Density graph. As indicated by the legend in the upper-right corner of the plot, the color scale mode range from blue (Minimum Percentage) to red (Maximum Percentage). Click in the field and use the down arrow to select either of the following: • Auto - (Default) If selected, the application will automatically and dynamically change the color scale on the Spectrum Density graph. • Manual - if selected, the user can manually set or change the Maximum Percentage and/or Minimum Percentage values. Highlight the existing Minimum Percentage and Maximum Percentage values and override them with new values. Once the Minimum Percentage and Maximum Percentage values are set, any values that fall outside the range will be ignored by the Spectrum Density plot. Those that are below the Minimum Percentage value will show as blue while those that are above the Maximum Percentage value will show as red on the Spectrum Density graph.
Maximum Percentage	Allows the user to set or change the maximum percentage value (shown on the right-hand side) of the color scale. It is 100 by default, but you can change this value to any value if you select Manual in the Color Scale Mode. Simply highlight the existing value and override it with a new value.
Minimum Percentage	The minimum percentage (shown on the left-hand side) of the color scale. It is 0 by default, but you can change it to any value between 0 and 100, if you select Manual in the Color Scale Mode. Simply highlight the existing value and override it with a new value.
Minimum Power	Allows the user to set or change the minimum power value in dBm in the Y-axis of the Spectrum Density graph. By default, the Minimum Power value is -120, but you can change it to any value as low as -140.
Peak Power	Allows the user to set or change the peak power value in dBm in the Y-axis of the Spectrum Density graph. By default, the Peak Power value is -20, but you can change it to any value less than 0 dBm. Highlight the existing Peak Power value and override with a new value.
Start Frequency	Allows the user to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	Allows the user to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

The text message at the bottom of the Spectrum Density Configuration dialog box changes with the parameter you select. It provides a brief description of the parameter being selected.

Spectrogram Graph

The Spectrogram graph provides another way to present the same data as shown in the Real-Time FFT graph. It allows you to visualize the changes in the spectrum over a period of time and to easily identify any shift in frequency use and the duration of such shifts. The X-axis shows the frequency range covered by the selected radio band. The Y-axis shows in real time the number of sweeps the spectrum adapter scans the RF spectrum, which ranges from 0 to 100. See Figure 6-8.

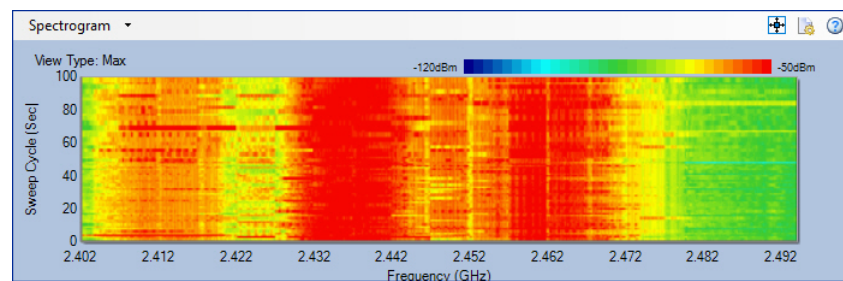


Figure 6-9: Spectrogram graph

Each time the adapter scans the RF spectrum makes one sweep cycle, which is represented by a horizontal (colored) line across the spectrogram plot. The spectrogram scrolls dynamically upward as the application scans the spectrum. New data appear at the bottom of the graph while old data are constantly pushed to the top. Since the plot can only display up to 100 sweep cycles, anything beyond 100 will be discarded.

The sweep cycle values are mapped to a range of colors which corresponds to color range shown in the color legend in the upper-right corner of the graph. Blue represents the Minimum power values while red represents the Maximum power values.

Configuring Spectrogram Graph Parameters

You can set or change the parameters of the Spectrogram graph using the Chart Configuration button.

To configure Spectrogram graph parameters:

- 1) From the upper-right corner of the Spectrogram graph, click  (Chart Configuration). The Spectrogram Configuration dialog box appears. See Figure 6-10.

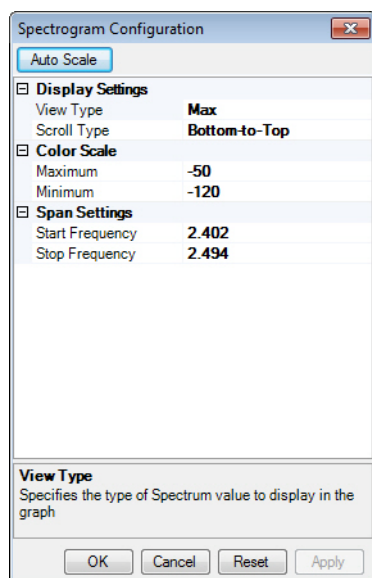


Figure 6-10: Configuring Spectrogram graph

- 2) Make the desired selections and/or entries as described in Table 6-4.
- 3) Click Apply and then OK.

Table 6-4: Configuring Spectrogram Graph Parameters

Parameter	Description
View Type	Allows the user to decide which type of spectrum data to be displayed in the Spectrogram graph. Click in the field and use the down arrow to select one of the following: • Current - plots Current power readings. • Average - plots the average power reading of the latest five sweeps. • Maximum - plots the maximum power reading of the latest five sweeps. • Duty Cycle - plots Duty Cycle readings.
Scroll Type	This option allows you to set the direction in which the graph scrolls (e.g., up or down).

Table 6-4: Configuring Spectrogram Graph Parameters

Parameter	Description
Maximum	Allows the user to set or change the maximum power value in dBm in the Spectrogram graph. By default, the Maximum Power value is -20, but you can change it to any value less than 0 dBm. The Maximum value appears on the right end of the color scale. Any value that exceeds the set maximum will appear in red. Highlight the existing Maximum value and override with a new value.
Minimum	Allows the user to set or change the minimum power value in dBm in the Spectrogram graph. By default, the Minimum Power value is -100 dBm, but you can change it to any value as low as -140. The Minimum value Specify the minimum value of the color scale, which can be equal to or greater than -140 dBm.
Starting Frequency	Allows the user to set or change the start point of a frequency range. Highlight the existing value and override it with a new value.
Stop Frequency	Allows the user to set or change the end point of a frequency range. Highlight the existing value and override it with a new value.

The text message at the bottom of the Spectrogram Configuration dialog box changes with the parameter you select. It provides a brief description of the parameter being selected.

Channel Power

The Channel Power graph shows the maximum and average power levels across all channels in the selected radio band. The X-axis shows all available channels for the selected radio band and the y-axis shows the rough energy readings. See [Figure 6-11](#).

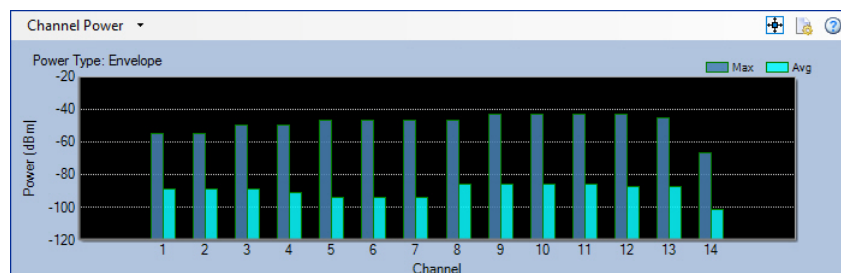


Figure 6-11: Configuring Channel Power graph

Channel Power Types

The Channel Power can be defined either as Envelope or Integrated. Envelope power is defined as the maximum, or peak, energy level in a channel's frequency range. Integrated power is similar, and is defined as the average power of all frequency power levels in a channel's frequency range. In the bar chart, the Max bar corresponds to the Max data line on the FFT chart, while the Avg bar corresponds to the Average data line on the FFT graph.

With the chart set to the Envelope power type, the Max bar will show the dBm power of the strongest received signal within the 20MHz channel frequency width as recorded by the Max data line in the FFT chart, while the Avg bar will show the highest dBm value of the Average data line for the same channel frequency width.

With the chart set to the Integrated power type, the application first samples the data from the Max and Average data lines in the FFT graph, then calculates the average power of all the sampled frequencies within the 20MHz channel frequency width. These values are then represented by the Max and Avg bars in the chart.

Note: If you place the cursor over a channel, a tooltip will pop up showing the Maximum and Average power readings on that channel.

Configuring Channel Power Graph Parameters

You can set or change the parameters of the Channel Power graph using the Chart Configuration button.

To configure Channel Power graph parameters:

- 1) From the upper-right corner of the Channel Power graph, click  (Chart Configuration). The Channel Power Configuration dialog box. See Figure 6-12.

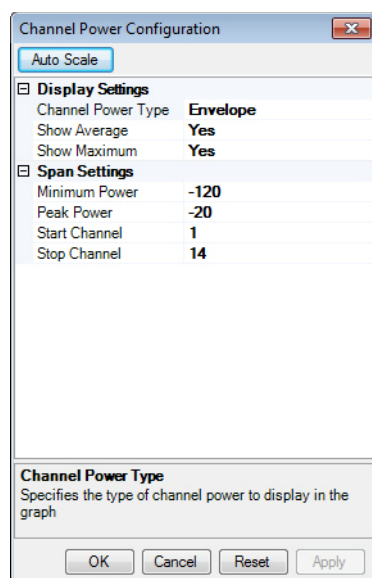


Figure 6-12: Configuring Channel Power graph

- 2) Make the desired selections and/or entries as described in Table 6-5.
- 3) Click Apply and then OK.

Table 6-5: Configuring Channel Power Graph Parameters

Parameter	Description
Show Average	Allows the user to show or hide the average power (aqua) readings in Channel Power graph. Click in the field and select one of the following: • Yes - shows the average power in the graph (default). • No - hide the average power in the graph.
Show Maximum	Allows the user to show or hide the maximum power (blue) readings in the graph. Click in the field and select one of the following: • Yes - shows the maximum power in the graph (default). • No - hide the maximum power in the graph.

Table 6-5: Configuring Channel Power Graph Parameters

Parameter	Description
Channel Power Type	Select one of the following: - Envelope - The highest energy reading that has been reached at a particular frequency with a frequency range. See the description at the beginning of this section. - Integrated - The total summation of energy reading of an entire frequency range. See the description at the beginning of this section.
Minimum Power	Allows the user to set or change the minimum power value in dBm in the Y-axis of the Channel Power graph. By default, the minimum power value is -120, but you can change it to any value as low as -140.
Peak Power	Allows user to set or change the peak power value in dBm in the Y-axis of the Channel Power graph. By default, the Peak Power value is -20, but you can change it to any value less than 0 dBm. Highlight the existing Peak Power value and override with a new value.
Start Channel	Allows the user to set the first channel in the range of channels to be selected. Highlight the existing value and override it with a new value.
Stop Channel	Allows the user to set the last channel in the range of channels to selected. Highlight the existing value and override it with a new value.

The text message at the bottom of the Channel Power Configuration dialog box changes with the parameter you select. It provides a brief description of the parameter being selected.

Channel Duty Cycle

The percentage of time that the RF energy is present in the channel above the noise floor. The duty cycle calculation is done by summing up the duration of all pulses that are detected within the bandwidth of a channel. There are actually two accumulators, one for pulses that are determined to be 802.11 pulses and another for pulses that are not 802.11 packets. The WLAN duty factor (or channel utilization as we refer to it) is computed by dividing the accumulated 802.11 WLAN pulse time by the time the radio was dwelling on that channel. The non-WLAN duty factor is computed by dividing the accumulated time of non-WLAN pulses with the total channel dwell time. See [Figure 6-13](#).

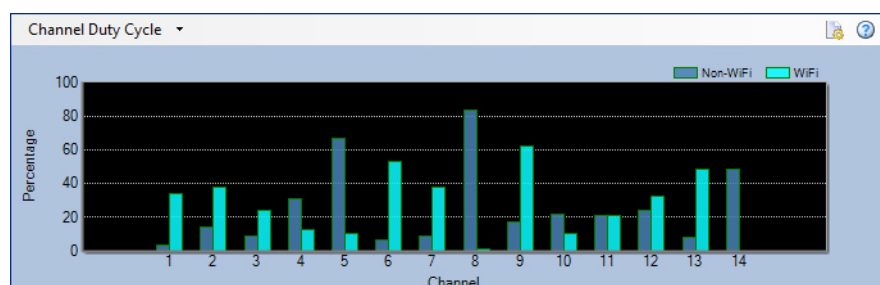


Figure 6-13: Channel Duty Cycle graph

Configuring Channel Duty Cycle Graph Parameters

You can set or change the parameters in the Channel Duty Cycle graph using the Chart Configuration button.

To configure Channel Duty Cycle graph parameters:

- 1) From the upper-right corner of the Channel Duty Cycle graph, click  (Chart Configuration). The Channel Duty Cycle Configuration dialog box. See Figure 6-14.

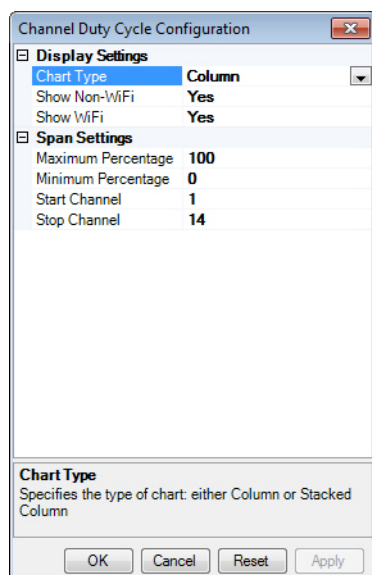


Figure 6-14: Configuring Channel Duty Cycle graph

- 2) Make the desired selections and/or entries as described in Table 6-5.
- 3) Click **Apply** and then **OK**.

Table 6-6: Channel Duty Cycle Graph Parameters

Parameter	Description
Chart Type	Toggles between column and stacked column displays. When viewing by stacked column, the data for WiFi and non-WiFi data will be displayed in a single column, with WiFi data stacked on top of the non-WiFi information.
Show Non-WiFi	Enables or disables display of non-wifi data.
Show WiFi	Enables or disables display of wifi data.
Maximum Percentage	Allows the user to specify the maximum percentage to be displayed in Channel Duty Cycle graph. Highlight the existing value and then override it with a new value.
Minimum Percentage	Allows the user to specify the minimum percentage to be displayed in Channel Duty Cycle graph. Highlight the existing value and then override it with a new value.
Start Channel	Allows user to set the first channel in the range of channels to be selected. Highlight the existing value and override it with a new value.
Stop Channel	Allows the user to set the last channel in the range of channels to selected. Highlight the existing value and override it with a new value.

Non-WiFi Devices

The Non-WiFi Devices table displays all non-WiFi devices that the application has detected in the network environment. The devices are organized in the following categories:

- Bluetooth Devices
- Digital Cordless Phones
- Analog Cordless Phones
- Wireless Cameras
- Microwave Ovens
- Baby Monitors
- Digital Video Monitors
- Wireless Game Controllers
- RF Jammers

- Zigbee Devices
- Non-Bluetooth Wireless Mouse
- Motion Detector
- Radar

Figure 6-15 shows the information contained in the Non-WiFi Devices table.

Name	Peak Power dBm	Avg Power dBm	Last Seen Channel	Affected Channels	Center Frequency GHz	Duty Cycle	First Seen
Type: Baby Monitor (3)							
Digital Baby Monitor (Id 52)	-49	-49	14	12..14	2.481	0.00	11/1/2011 11:11:11 AM
Digital Baby Monitor (Id 51)	-53	-53	14	12..14	2.481	36.53	11/1/2011 11:11:11 AM
Digital Baby Monitor (Id 50)	-54	-54	14	12..14	2.481	0.00	11/1/2011 11:11:11 AM

Figure 6-15: Non-WiFi Devices

The Non-WiFi Devices table shows the following information about each non-WiFi device that are listed:

- **Name (Device Type)** - The device category a device belongs to (refer to the bullet list above).
- **Peak Power dBm** - The highest energy reading in dBm ever recorded of device.
- **Avg Power dBm** - The average energy reading in dBm of the device.
- **First Seen Time** - The time when the device was detected for the first time.
- **Last Seen Time** - The most recent time when the device was detected.
- **Event Count** - The number of times the device was detected (refer to the Event Spectrogram)
- **Last Seen Channel** - The channel on which the device was last detected.
- **Affected Channels** - Channels that are affected by the device.
- **Center Frequency GHz** - The center frequency used by the device.
- **Duty Cycle** - The percentage of time that the RF energy is present in the channel above the noise floor.
- **Is Active** - Indicates if the device is active or not. You'll see a check mark if it is active, or a cross mark if otherwise.
- **Is Hopping** - Indicates if the device is a frequency-hopping device. You'll see a check mark if it is a frequency-hopping device, or a cross mark if it is otherwise.

Event Spectrogram

The Event Spectrogram provides a visual presentation of real-time information about events (device detections) that the application has made in the network. Each detection is an event which is represented by a color band. The color of the band indicates the signal strength of the device being detected (refer to the signal scale on top of the graph). If more detections are made of the same device as the application sweeps the spectrum, the band will become thicker (taller). The height of the color band indicates the (length of time in seconds the device has been detected. It stops increasing when the device becomes inactive (meaning that the device has not been detected for a minute). The width of the line/band indicates the channels or frequencies being affected by the device. If the device is a frequency-hopping device, then the line/band may extend sideways as the device hops from one channel to another.

Figure 6-16 shows the Event Spectrogram.

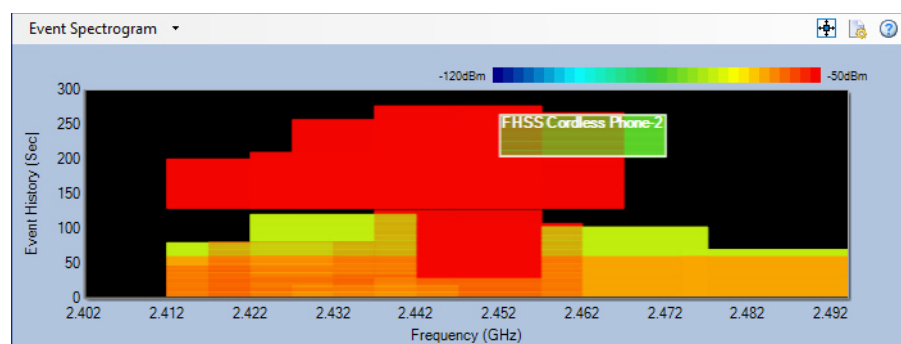


Figure 6-16: Event Spectrogram

If you place the cursor over the line/band, a tooltip will pop up showing some basic information about that device, such as the type of the device, its peak power, and the time of it being detected.

Configuring Event Spectrogram

In the upper-right corner of the plot is a configuration button which allows you to configure and change a number of parameters in the Event Spectrogram plot.

To set or change parameters in the Event Spectrogram plot:

- 1) Click the Chart Configuration button in the upper-right corner. The Event Spectrogram Configuration dialog box opens. See [Figure 6-17](#).

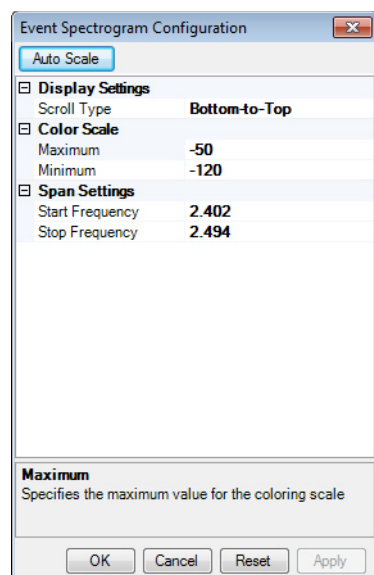


Figure 6-17: Configuring Event Spectrogram

- 2) Make the desired changes to the following parameters:
 - Maximum - The maximum energy level to show in the Event Spectrogram, which is on the red end of the color legend.
 - Minimum - The minimum energy level to show in the Event Spectrogram, which is on the blue end of the color legend.
 - Start Frequency - The lowest frequency of the frequency range.
 - Stop Frequency - The highest frequency of the frequency range.
- 3) Click OK when done

Interference Power

The Interference Power chart provides a quick display of all devices, both WiFi and non-WiFi, that are causing potential interference in the wireless spectrum. Using this function, users can quickly identify which channels are experiencing unusually high levels of network interference and plan or adjust the deployment accordingly. See [Figure 6-18](#).

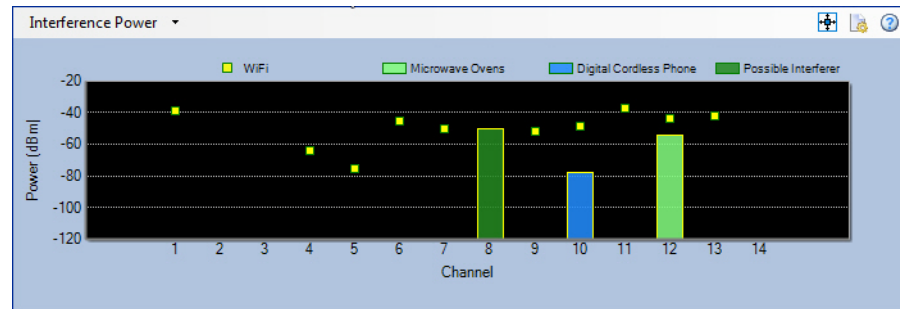


Figure 6-18: Interference Power Chart

As noted in the color legend above the main portion of the chart, the yellow points on the graph represent the current signal strength of the strongest AP detected on each channel; hovering over the point provides the device's name and MAC address. The point's location on the chart indicates the level of interference that it is experiencing; as the interference level climbs, the device's performance can suffer as a result.

Non-WiFi devices are color-coded to make it easy for users to quickly assess which devices are present at any given time. Hovering over the color bar of a given interferer provides a pop-up display that indicates the level of interference caused by the device as well as the device's type (if known).

Configuring the Interference Power Display

In the upper-right corner of the plot is a configuration button which allows you to configure and change a number of parameters in the Interference Power plot.

To set or change parameters in the Interference Power plot:

- 1) Click the Chart Configuration button in the upper-right corner. The Interference Power Configuration dialog box opens. See [Figure 6-19](#).

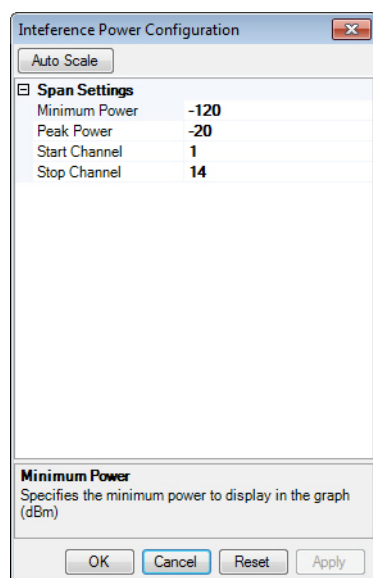


Figure 6-19: Configuring Interference Power

- 2) Make the desired changes to the following parameters:
 - Minimum Power – The minimum power level that will be displayed on the graph.
 - Peak Power – The maximum power level that will be displayed on the graph.
 - Start Channel – The first channel that will be displayed.
 - Stop Channel – The last channel that will be displayed.
- 3) Click OK when done

Channel Duty Cycle vs Time

The Channel Duty Cycle vs Time graph shows the recorded duty cycle over the course of time, allowing the user to easily identify channels that are experiencing a high percentage of traffic steadily over for an extended period. The X-axis shows the amount of time elapsed and the Y-axis displays the duty cycle percentage. See [Figure 6-20](#).

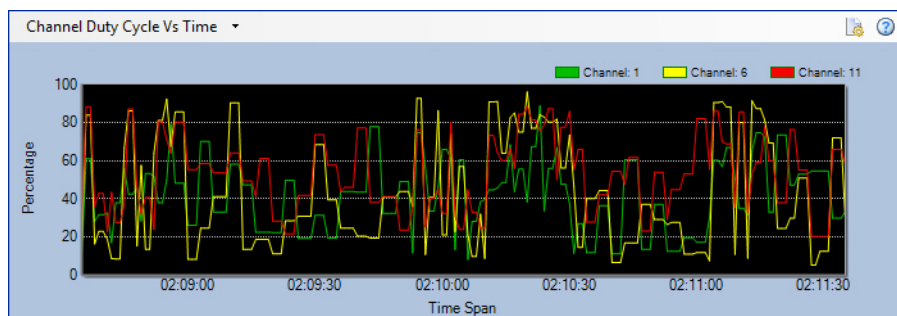


Figure 6-20: Channel Duty Cycle vs Time graph

As shown above, the graph will display up to three channels at a time in color-coded lines. The channels can be modified via the chart configuration, as discussed below.

Configuring Channel Duty Cycle vs Time

You can set or change the parameters in the Channel Duty Cycle vs Time graph using the Chart Configuration button.

To configure Channel Duty Cycle vs Time graph parameters:

- 1) From the upper-right corner of the graph, click  (Chart Configuration). The Channel Duty Cycle vs Time Configuration dialog box appears. See [Figure 6-21](#).

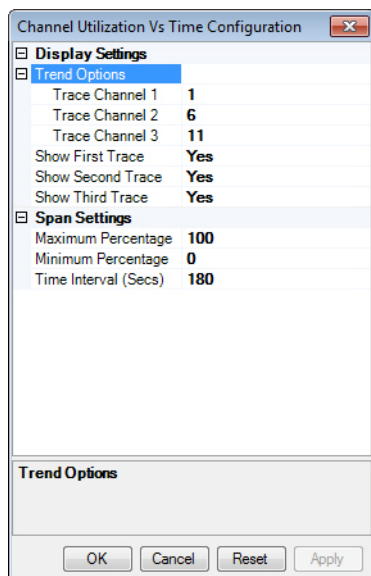


Figure 6-21: Configuring Channel Duty Cycle vs Time graph

- 2) Make the desired selections and/or entries as described in Table 6-5.

3) Click **Apply** and then **OK**.

Table 6-7: Channel Duty Cycle vs Time Graph Parameters

Parameter	Description
Trend Options	Use these fields to specify the channels that should be displayed in the graph. Users can select up to three channels at any single time.
Show First/Second/Third Trace	These fields activate or deactivate the trace options specified in the first portion of the configuration. Select 'Yes' to activate (e.g., display) each trace as needed. Selecting 'No' will remove the trace from the graph.
Maximum Percentage	Allows the user to specify the maximum percentage to be displayed in the graph. Highlight the existing value and then override it with a new value.
Minimum Percentage	Allows the user to specify the minimum percentage to be displayed in the graph. Highlight the existing value and then override it with a new value.
Time Interval (Secs)	The maximum number of seconds that will be displayed on the chart at any given time.

Interference Power vs Time

The Interference Power vs Time graph provides a visual representation of the length of time in which interferers are active. Note that this graph displays non-WiFi interference only, and can help users identify non-802.11 interferers that are active consistently over time.

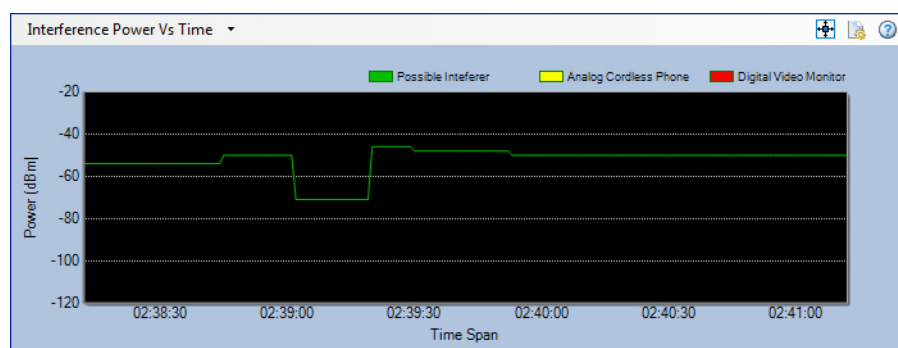


Figure 6-22: Interference Power vs Time

By default, the graph is set to display interferers separated into individual channels, allowing the user to troubleshoot problems on up to three channels at a time. This configuration can be modified, however, to display lines for each interferer present instead, making it significantly easier to identify multiple sources of interference as well as their impact on the network. Hovering over the lines in the graph provides additional details regarding the information displayed, including interference level and the type of interferer (if known).

Configuring the Interference Power vs Time Graph

As mentioned above, the configuration menu for the Interference Power vs Time graph allows the user to alternate between displaying interference data by channel and by device type. Refer to Table 6-8 for specific options that can be configured in the graph, as shown below.

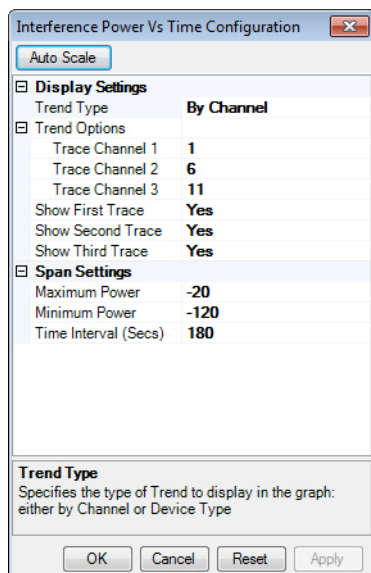


Figure 6-23: Interference Power vs Time Configuration

Table 6-8: Interference Power vs Time Graph Parameters

Parameter	Description
Trend Type	Select whether to display data by channel or by device as desired.
Trend Options	Depending on the selection made in the Trend Type field, these fields allow the user to select the channels or devices that should be displayed.
Show First/ Second/Third Trace	These fields activate or deactivate the trace options specified in the first portion of the configuration. Select 'Yes' to activate (e.g., display) each trace as needed. Selecting 'No' will remove the trace from the graph.
Maximum Power	Allows the user to specify the maximum power to be displayed in the graph. Highlight the existing value and then override it with a new value.
Minimum Power	Allows the user to specify the minimum power to be displayed in the graph. Highlight the existing value and then override it with a new value.
Time Interval (Secs)	The maximum number of seconds that will be displayed on the chart at any given time.

BlueSweep Integration

BlueSweep software is designed to identify nearby devices with Bluetooth wireless technology and alert users to potential Bluetooth security risks. It identifies and tracks devices up to 300 feet away and lets users know what their own Bluetooth devices are doing. BlueSweep runs on laptop computers that support Windows XP.

Additional Bluetooth Analysis

AirMagnet Spectrum XT offers enhanced Bluetooth interferer information using an optional Windows-compatible Bluetooth adapter. The enhanced information includes details on the name, ID, services, etc. for Bluetooth devices.

Users can either use the Bluetooth adapter that is built into their PC or can use an external adapter. One such Bluetooth adapter is the IOGEAR GBU421 Bluetooth Adapter that has been tested by Airmagnet.

Note: It is recommended that users always use the Microsoft driver for Bluetooth devices instead of the vendor-supplied driver. The driver is built into Windows XP (SP3), Vista, and 7 operating systems. Please refer to Microsoft's website for obtaining drivers for other operating systems.

Caution: For effective customized signature detection and classification, it is recommended that the user not insert the optional Bluetooth adapter at the same time.

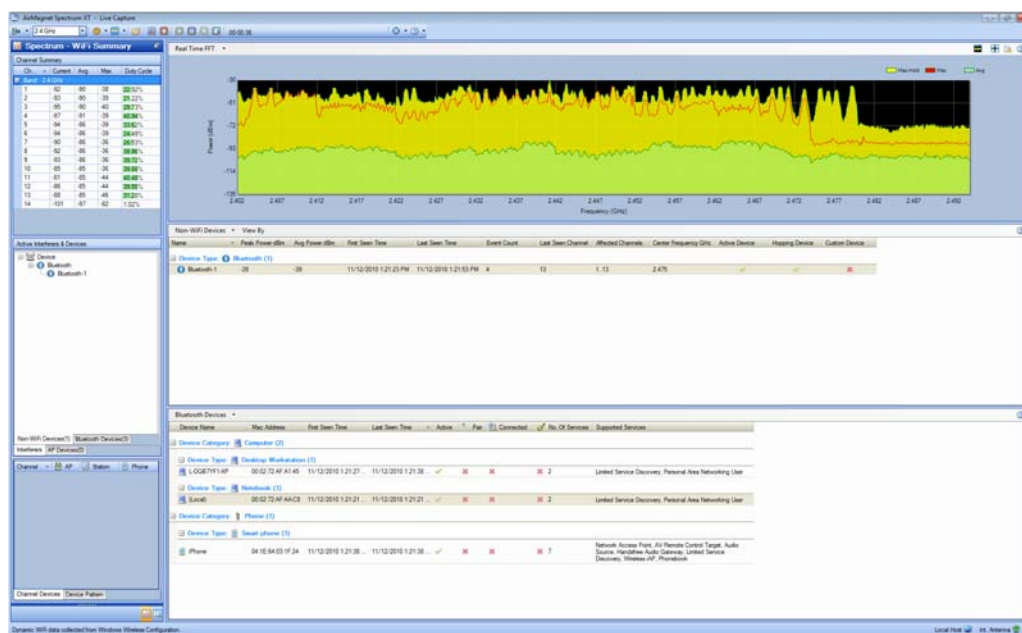


Figure 6-24: BlueSweep Integration Screen

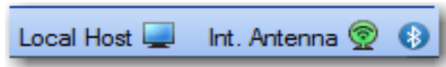


Figure 6-25: BlueSweep Active Setting

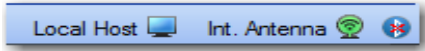


Figure 6-26: BlueSweep Inactive Setting

Chapter 7: Analyzing WiFi Data

Chapter Summary

This chapter discusses in detail the various WiFi graphs that AirMagnet Spectrum XT offers. It describes the data contained in each of these graphs and the ways to use them to analyze WiFi traffic on your network. It covers the following topics:

- WiFi graph options
- WiFi Devices table
- AP Signal Strength graph
- Channel Occupancy graph
- Channels by Speed graph
- Channels by Media graph
- Channels by Address graph
- Channel Utilization graph
- Top 10 APs by Speed
- Top 10 Active APs' Retry/CRC
- Channel Signal/Noise Ratio
- Channels by Retry/CRC

WiFi Graph Options

AirMagnet Spectrum XT has the capability to capture live WiFi data in real time and display them in charts or tables. This feature is a great complement to AirMagnet Spectrum XT's spectrum analysis capability, offering a complete, one-stop solution for detecting and troubleshooting various performance issues in the wireless network.

However, it must be noted that an AirMagnet-supported external wireless network adapter is required in order for AirMagnet Spectrum XT to capture live WiFi data in the network and presents them on its user interface. This means that the user must have both the AirMagnet Spectrum USB adapter and a supported external wireless network adapter running simultaneously on the same PC. Without a supported wireless network adapter, the application will be unable to capture live WiFi data in the network and presents them on its user interface.

For a list of supported wireless network adapters, refer to ["Supported Wireless Network Adapters" on page 8](#).

All WiFi graphs are listed in the WiFi Graphs list menu, which is available in all individual graphs.

To access the WiFi Graphs list menu:

- 1) From graph window, click the title of a graph.
- 2) From the drop-down menu, select WiFi Graphs. See Figure 7-1.

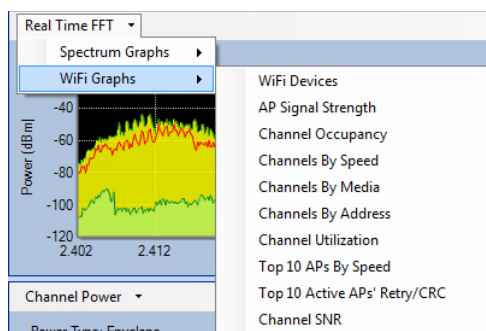


Figure 7-1: WiFi Graph options

As shown in Figure 7-1, the WiFi Graphs list menu contains all WiFi graphs AirMagnet Spectrum XT can generate. You can display any of them simply by clicking the option of your choice.

If no AirMagnet-supported WiFi adapter is present in the machine, only the first three graph selections will be available.

WiFi Devices Graph

The WiFi Devices graph (or table to be more exact) option shows all WiFi devices that AirMagnet Spectrum XT has detected on all available channels in the selected radio band. The devices are displayed by channel. Like the Channel Usage section, channels with no devices detected on them will not be listed in the WiFi Devices table. Within the same channel, the devices are then organized in three groups: AP, Station, and Phone. If no device has been detected for a certain group, then the group will not be listed either. See Figure 7-2.

Device/MAC	MAC Address	SSID	Signal dBm	Noise dBm	Security	First Frame Time	Last Frame Time	AP Name
Channel: 1 (11)								
Device Type: Station [3]								
Apple:42:5C:96	00:21:E9:42:5C:96	Air2	-66	-95	Encryp...	11/19/2008 10:35:06 ...	11/19/2008 10:42:29 ...	AP-10(BG)
Apple:8C:E6:67	00:21:E9:8C:E6:67		-100	-96	802.1x	11/19/2008 10:35:43 ...	11/19/2008 10:41:42 ...	AP-10(BG)
Hon Hai:A7:68:59	00:1C:26:A7:68:59	Amicus_G1_randomssidhuloffauto...	-100	-96	Encryp...	11/19/2008 10:34:37 ...	11/19/2008 10:42:15 ...	Unknown
Device Type: AP [8]								
AP-10(BG)	00:14:69:F3:16:30	Air2	-74	-95	WPA2-...	11/19/2008 10:34:40 ...	11/19/2008 10:42:29 ...	AP-10(BG)
AP-10(BG)	00:14:69:F3:16:31	AirMagnetGuest	-74	-95	WPA-...	11/19/2008 10:34:40 ...	11/19/2008 10:42:29 ...	AP-10(BG)
Cisco-Linksys:95:48...	00:10:7E:95:48:E9	linksys	-76	-95	Open	11/19/2008 10:34:37 ...	11/19/2008 10:42:29 ...	Cisco-Linksys:95...
Edimax:08:0C:C4	00:1F:1F:08:0C:C4	anygate	-100	-96	Encryp...	11/19/2008 10:34:39 ...	11/19/2008 10:42:28 ...	Edimax:08:0C:C4
QA_VoFL_2	00:0F:34:A7:78:10	QACiscoVoice	-90	-95	Encryp...	11/19/2008 10:34:40 ...	11/19/2008 10:42:29 ...	QA_VoFL_2
QA_VoFL_2	00:0F:34:A7:78:11	QASpectralink	-90	-95	WPA-...	11/19/2008 10:34:40 ...	11/19/2008 10:42:29 ...	QA_VoFL_2
QA_VoFL_2	00:0F:34:A7:78:12	QAVoFL	-91	-95	WPA2-...	11/19/2008 10:34:41 ...	11/19/2008 10:42:29 ...	QA_VoFL_2
QA_VoFL_2	00:0F:34:A7:78:13	QAVocera	-91	-95	Encryp...	11/19/2008 10:34:40 ...	11/19/2008 10:42:29 ...	QA_VoFL_2
Channel: 3 (1)								
Device Type: AP [1]								
Netgear:9E:85:48	00:18:4D:9E:85:48	chopper	-68	-91	Encryp...	11/19/2008 10:34:37 ...	11/19/2008 10:42:30 ...	Netgear:9E:85:48
Channel: 4 (3)								
Device Type: AP [3]								
AP-12(BG)	00:11:5C:4D:E8:F0	Air2	-90	-92	WPA2-...	11/19/2008 10:34:37 ...	11/19/2008 10:42:30 ...	AP-12(BG)
AP-12(BG)	00:11:5C:4D:E8:F1	AirMagnetGuest	-92	-92	WPA-...	11/19/2008 10:34:37 ...	11/19/2008 10:42:30 ...	AP-12(BG)
Symbol:9E:A7:29	00:A0:F8:9E:A7:29	qa_symbol@QA_lab_in_sunnyvale_hq	-73	-91	Open	11/19/2008 10:34:37 ...	11/19/2008 10:42:30 ...	Symbol:9E:A7:29
Channel: 6 (7)								
Device Type: AP [7]								
Cisco-Linksys:0F:8...	00:1D:7E:0F:8B:F0	linksys-gtv	-82	-96	Open	11/19/2008 10:34:37 ...	11/19/2008 10:42:30 ...	Cisco-Linksys:0F:...
QA-1200-50	00:14:6A:F0:64:A0	QA-1200-25	-91	-97	Encryp...	11/19/2008 10:34:37 ...	11/19/2008 10:42:26 ...	QA-1200-50

Figure 7-2: WiFi Devices

The WiFi Device graph provides comprehensive data about each WiFi device that AirMagnet Spectrum XT has detected in the network. Table 7-1 briefly describes the data contained in the WiFi Devices graph.

Table 7-1: WiFi Device Data

Data	Description
Device/MAC	This can be a device's name or MAC address, or a combination of device vendor name and partial MAC address (depending on the option selected using Settings>General>WiFi Devices)
MAC Address	A device's MAC address
SSID	A device's SSID
Signal dBm	A device's signal strength in dBm
Noise dBm	A device's noise level
Security	The security mechanism used on a device
First Frame Time	The time the first frame involving a device was detected.

Table 7-1: WiFi Device Data

Data	Description
Last Frame Time	Last Frame Time - The time the last frame involving a device was detected.
AP Name	The name of the AP itself or of the AP that provides service to a station or phone.

Since the WiFi Devices graph contains a great deal of data that require a lot of screen space, you may need to custom AirMagnet Spectrum XT's user interface in a way to make it easy for you to view WiFi device data. You can custom your screen space by doing either or both of the following, depending on your screen resolution:

- Hide the entire Spectrum-WiFi Summary section by clicking  (AutoHide).
- From the toolbar, click **Settings** and then uncheck (hide) all the graphs except for the one that corresponds to the WiFi Devices graph.

The order in which data are presented in WiFi Devices graph can be changed as well. All you need to do is to drag and drop, one at a time, the title of a column to where you want it to be.

AP Signal Strength Graph

The AP Signal Strength graph displays up to three APs with the strongest signal strength readings on each channel in the selected radio band. The X-axis shows all available channels in the radio band, and the Y-axis shows AP signal strength readings in dBm. See Figure 7-3.

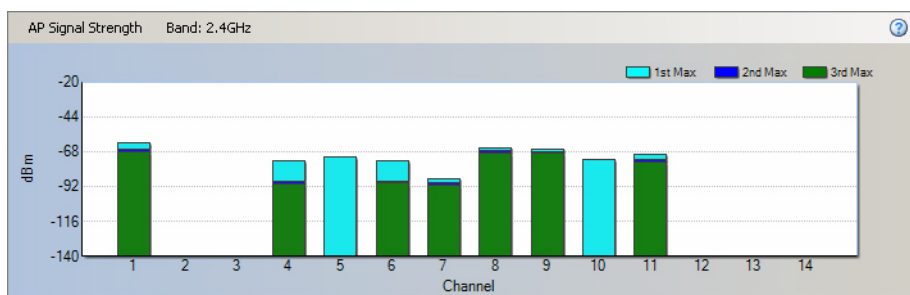


Figure 7-3: AP Signal Strength graph

As shown in Figure 7-3, the three highest AP signal strength readings are color-coded. Table 7-2 describes the color schemes used in the AP Signal Strength graph.

Table 7-2:

Color	Data	Description
Aqua	1st Max	The highest AP signal strength detected.
Blue	2nd Max	The second highest AP signal strength.
Green	3rd Max	The third highest AP signal strength.

If you place the cursor over a portion of a channel bar marked by any of the colors, a tip screen will appear showing the information about the AP. See Figure 7-4.

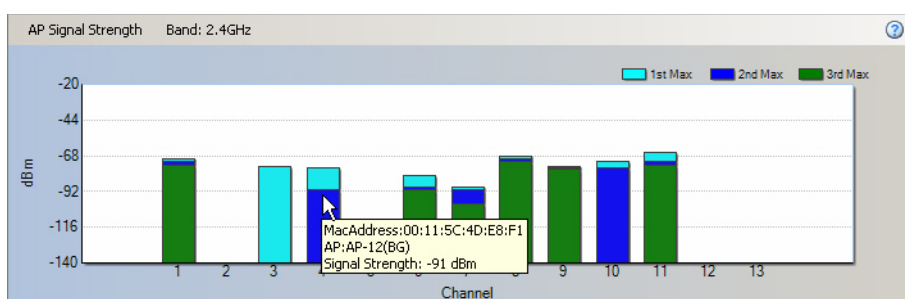


Figure 7-4: Viewing AP signal strength from tip screen

As shown in Figure 7-4, the tip screen provides the following basic information about the AP covering the part of bar chart where the cursor points,

- **MAC Address** - The MAC address of the AP.
- **AP** - It can be an AP's name, the combination of an AP's vendor name and part of its MAC address, or an AP's MAC address (depending on the option you have selected using **Settings>General>WiFi Devices**).
- **Signal Strength** - The signal strength of the AP being recorded.

*When a specific channel in the Channel Summary pane (in the upper-left corner of the screen) is selected, all channel bars in the graph will become tinted except the one corresponding to the channel being selected. This will help the user focus on the channel being selected. You can find more information about APs on any of these channels by selecting **WiFi Graphs>WiFi Devices** from the drop-down list menu in the upper left corner of the graph.*

Channel Occupancy Graph

The Channel Occupancy graph shows all the available channels for the selected radio band and which APs are occupying which channels. See Figure 7-5.

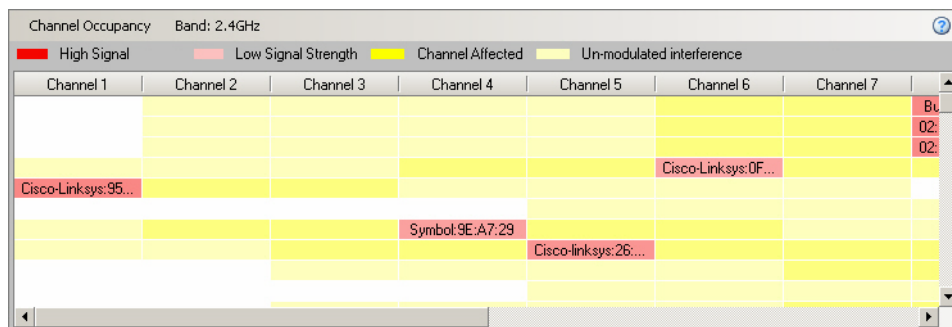


Figure 7-5: Channel Occupancy graph

As seen from the illustration above, each column in the Channel Occupancy graph represents a channel in the selected radio band, and each row represents an AP that has been detected. The fields are marked by four different colors that convey their designated meanings, as described in Table 7-2.

Table 7-3: Channel Occupancy Graph Color Scheme

Color	Data
Red	Center frequencies of APs identified by name or SSID. The dark shade of red indicates strong AP signal strength.
Light Red	Center frequencies of APs identified by name or SSID. The light shade of red indicates that weak AP signal strength.
Yellow	Channels affected by the modulated inference from APs in the center frequencies.
Light Yellow	Channels affected by unmodulated interference from APs in the center frequencies.

Based on the information presented on the screen, the user can then reallocate their APs to optimize their performance. The information is very helpful for making AP channel allocation decisions to optimize AP performance.

Modulated interference refers to interference that occurs within a device's modulated spectrum (i.e., within the device's operating channel width), whereas unmodulated interference refers to interference caused by the "bleed over" of signals beyond the modulated portion of the transmission.

Like the WiFi Devices graph, the Channel Occupancy graph requires more screen space to display its content. Therefore, you may need to custom AirMagnet Spectrum XT's user interface in a way to make it easy for you to view the data. You can custom your screen space by doing either or both of the following, depending on your screen resolution:

- Hide the entire Spectrum-WiFi Summary section by clicking  (AutoHide).
- Click **Settings** and then uncheck all graphs except for the one that corresponds to the Channel Occupancy graph.

Channels by Speed

The Channels by Speed graph displays the relative amount of data (in kilobytes) that has been transmitted at each data rate on each available channel in the selected radio band. The X-axis shows all available channels in the radio band and the data rate used on each channel, whereas the Y-axis shows the amount of the data (in kilobytes) transmitted on each channel as well as a visual breakdown by data rate of the volume of data being transmitted. See Figure 7-6.

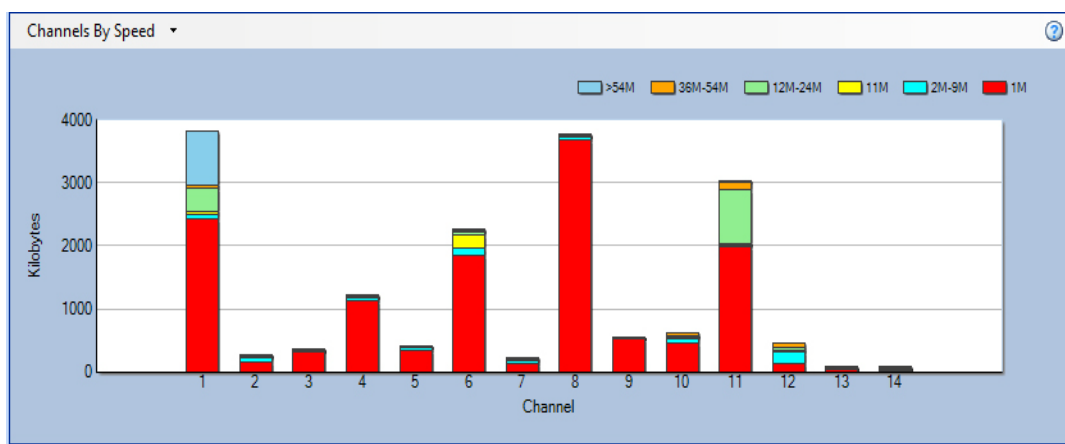


Figure 7-6: Channels by Speed graph

The applicable transmission rates used in the selected radio band are colored coded. Table 7-3 briefly describes the color scheme.

Table 7-4: Color Scheme for Transmission Rates

Color	Transmission Rate (in Mbps)
Blue	.11n (for 802.11n devices)
Orange	36~54
Green	12~24
Yellow	11
Aqua	2~9
Red	1

If you place the cursor over a particular channel, a tip screen will appear providing some brief statistics of the amount data transmitted at the various transmission rates used on that channel.

Channels by Media

The Channels by Media graph shows that volume of WiFi transmissions in kilobytes recorded on each channel in the selected radio band. It also provides a rough breakdown by 802.11 media type of the transmission on each channel. The X-axis shows all available channels in the selected band and the types of media used for the transmission; the Y-axis shows the volume of transmission in kilobytes. See Figure 7-7.

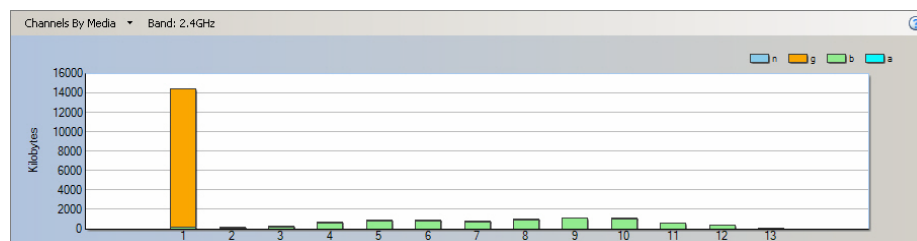


Figure 7-7: Channels by Media graph

Each bar in the Channels by Media graph represents the total amount of data in kilobytes that has been transmitted on a channel. The WiFi traffic is categorized by the type of 802.11 media being used. The media are color-coded, with each color representing a specific type of 802.11 media. Table 7-5.

Table 7-5: Color Scheme for 802.11 Media Types

Color	Media Type
Blue	802.11n
Orange	802.11g
Green	802.11b
Aqua	802.11a

If you place the cursor over a channel, a tip screen will pop up showing the volume of data transmitted using each type of media. See Figure 7-8.

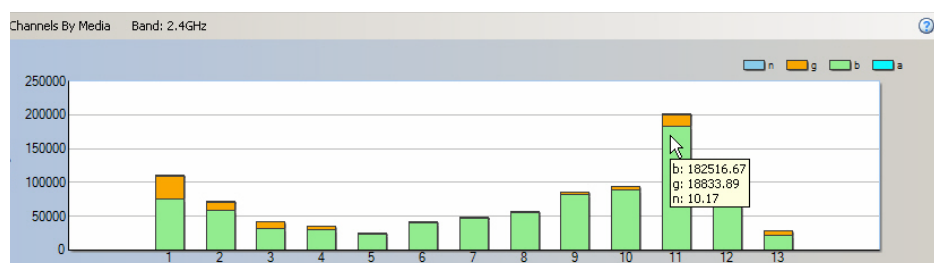


Figure 7-8: Tip screen showing transmission by media

Channels by Address

The Channels by Address graph shows the volume of data transmission in kilobytes that has been recorded on each channel in the selected radio band. It also provides a rough breakdown of the transmission by the type of address (i.e., broadcast, multicast, and unicast) that was used for the transmission. The X-axis shows the available channels and the type of address on each channel; the Y-axis shows the volume of data in kilobytes being transmitted. See Figure 7-9.

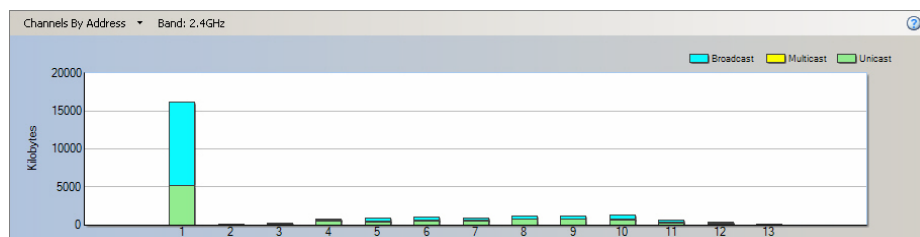


Figure 7-9: Channels by Address graph

As shown in Figure 7-9, three types of addresses can be used for network traffic. The addresses are coded in distinctive colors, which are described in Table 7-6.

Table 7-6: Color Scheme for Channels by Address Graph

Color	Address	Description
Aqua	Broadcast	The process of sending the same data to all stations on the network.
Yellow	Multicast	The process of sending a single message to multiple destinations simultaneously. It is a one-to-many transmission similar to broadcasting, except that multicasting means transmission to specific groups, whereas broadcasting implies sending to everybody. Multicasting can save considerable bandwidth when sending large volumes of data because the bulk of the data is transmitted once from the source through major backbones and are multiplied, or distributed out, at switching points closer to the recipients.
Green	Unicast	The process of sending duplicates of the same message to multiple destinations on the network. In unicast, even though multiple users might request the same data from the same server at the same time, duplicate data streams are transmitted, one to each destination.

If you place the cursor over a channel, a tip screen will pop up showing the volume of transmission carried by each address type. See Figure 7-10.

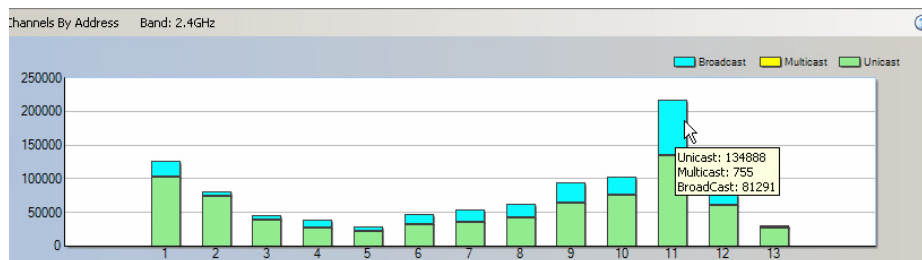


Figure 7-10: Tip screen showing transmission by address

Channel Utilization

The Channel Utilization graph shows the percentage of bandwidth being used on each channel and the breakdown of the utilization by transmission rate. The X-axis shows all available channels for the selected radio band as well as the transmission rates being used on each channel; the Y-axis shows the overall percentage of bandwidth being used on each channel. See Figure 7-11.

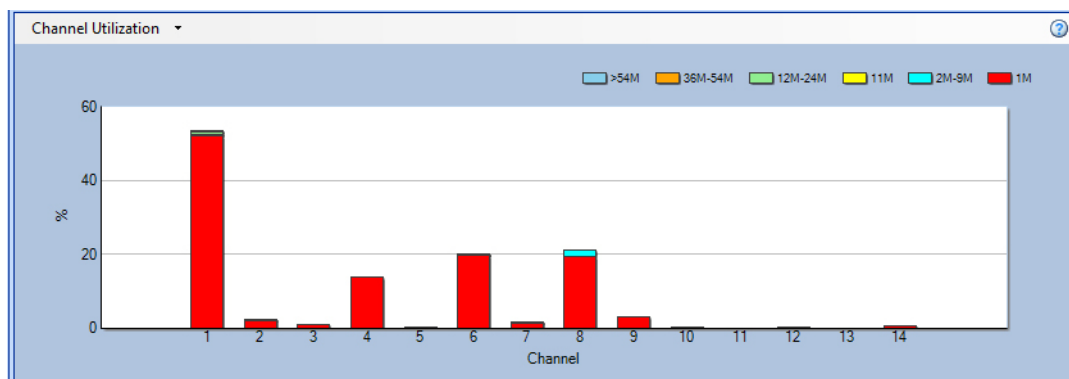


Figure 7-11: Channel Utilization graph

Each bar in the Channels Utilization graph represents the percentage of bandwidth being used on each channel. It also shows the breakdown of the utilization by transmission rate. The various transmission rates are coded, as described in Table 7-7.

Table 7-7: Color Scheme for Channel Utilization Graph

Color	Transmission Rate (in Kilobytes)
Blue	.11nM (for all 802.11n transmissions)
Orange	36~54
Green	12~24
Yellow	11
Aqua	2~9
Red	1

If you place the cursor over a channel, a tip screen will pop up showing the breakdown of channel bandwidth utilization by transmission rate. See Figure 7-12.

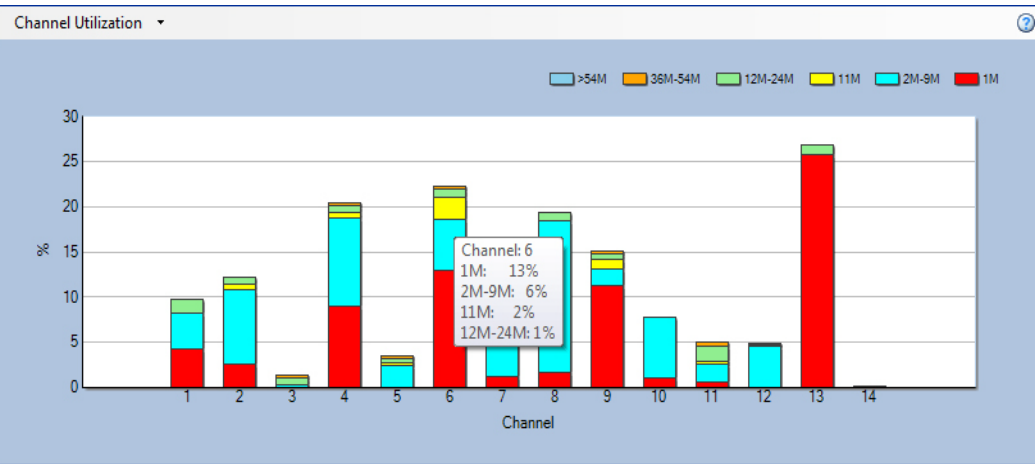


Figure 7-12: Viewing channel bandwidth breakdown by data rate

Top 10 APs by Speed

The Top 10 APs by Speed graph shows the 10 APs that have transmitted the most amount of data (in kilobytes) as well as the breakdown of the transmissions by data rate on each AP. The X-axis shows the names of the top 10 APs and the transmission rates being used by the APs; the Y-axis shows the volume of data in kilobytes being recorded. See Figure 7-13.

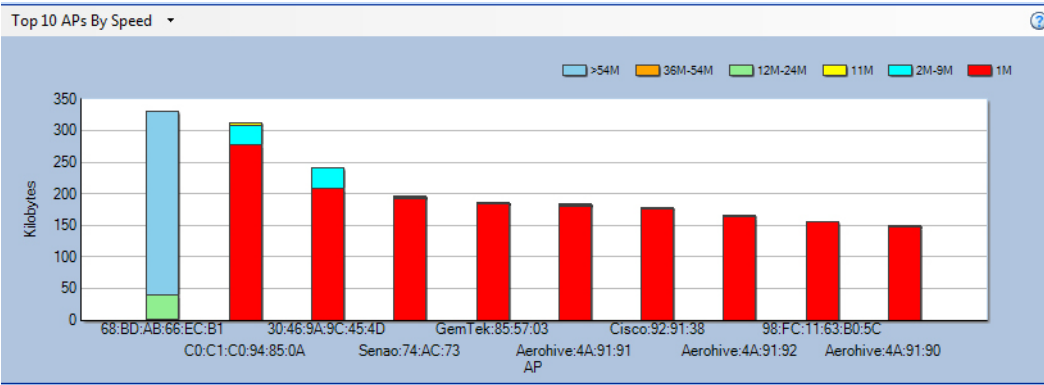


Figure 7-13: Top 10 APs by Speed graph

Each bar in the Top 10 APs by Speed graph represents the volume of data transmission being recorded involving a specific AP. It also provides a breakdown of the transmission by transmission rate. The various transmission rates are coded, as described in Table 7-8.

Table 7-8: Color Scheme for Top 10 APs by Speed Graph

Color	Transmission Rate (in Kilobytes)
Blue	.11nM (for all 802.11n transmissions)
Orange	36~54
Green	12~24
Yellow	11
Aqua	2~9
Red	1

If you place the cursor over a bar, a tip screen will pop up showing the breakdown of the volume of transmission by transmission rate by that AP. See Figure 7-14.

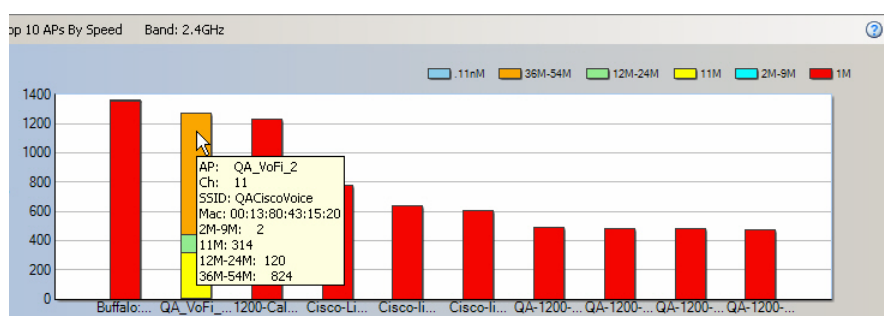


Figure 7-14: Viewing AP transmission breakdown by data rate

The tip screen also shows some basic information about the AP, such as its name or IP address, the channel it is using, its SSID, and its MAC address.

Top 10 Active APs' Retry/CRC

The Top 10 Active APs' Retry/CRC graph shows the percentage of packets that are either Retry or CRC packets for the top 10 APs that are transmitting the most data. The X-axis display APs that have been detected and the types of packets being transmitted (Retry vs. CRC); the Y-axis shows the percentages of Retry and/or CRC packets. See Figure 7-15.

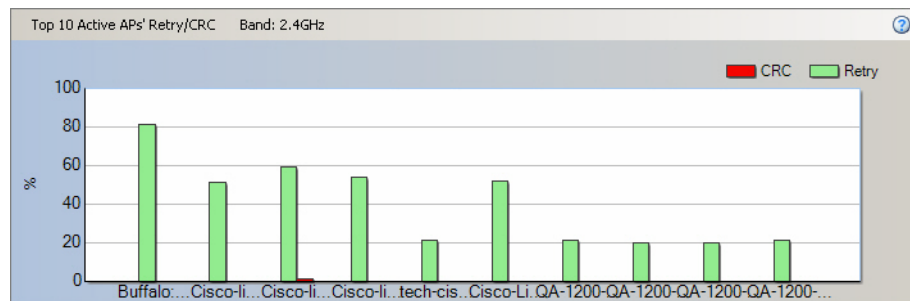


Figure 7-15: Top 10 Active APs' Retry/CRC

As shown in Figure 7-15, the CRC and Retry packets are color-coded, with red for CRC and green for Retry. The APs are identified by name, IP address, or whatever identification is used on the network. If you place the cursor on an AP, a tip screen will pop up showing some basic information about the AP and the percentages of Retry and CRC packets transmitted by the AP. See Figure 7-16.

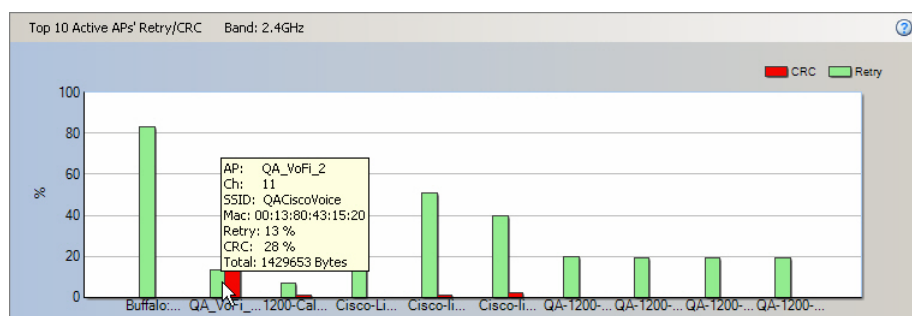


Figure 7-16: Viewing AP Retry/CRC transmission percentage

Channel Signal/Noise Ratio

The Channel Signal/Noise Ratio graph shows the ratio of signal to noise present on each displayed channel. The X-axis shows the list of selected channels while the Y-axis displays the ratio in terms of dB. See Figure 7-17.



Figure 7-17: Channel SNR Graph

Channels by Retry/CRC

The Channels by Retry/CRC graph shows the percentage of traffic present on each channel composed of Retry and Cyclic Redundancy Check (CRC) packets. The X-axis shows the list of selected channels while the Y-axis displays the percentage level. As shown in the color legend, Retry traffic is displayed in green while red represents CRC transmissions. See Figure 7-18.

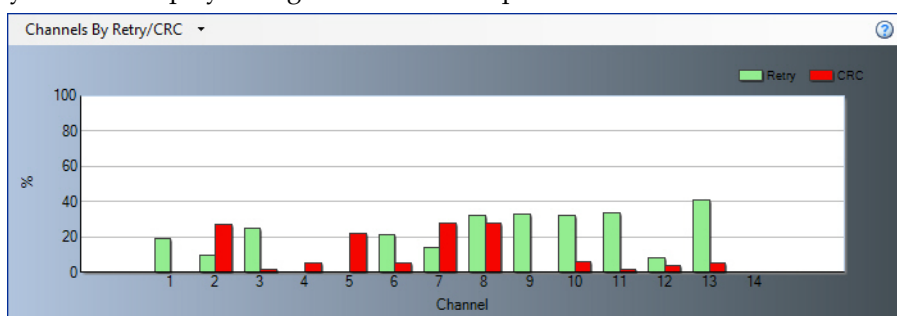


Figure 7-18: Channels by Retry/CRC

Chapter 8: Finding Devices

Chapter Summary

This chapter discusses how to use the Find Device tool to physically locate various spectrum devices that the application has detected on your network. It covers the following topics:

- Find Device Screen UI Components
- Event Log
- Device Details
- Device Pattern
- Find Device Tool
- Device Description
- Finding Devices on the Network

Find Device Screen UI Components

AirMagnet Spectrum XT comes with a robust Find Device tool that enables you to find any device (WiFi or non-WiFi) detected in your network. You can access this tool either by clicking  (Find Device) in the lower left part of the screen or by double-clicking a device in the Device List on the Spectrum-WiFi Summary screen. The former enables you to switch to the Find Device screen where you can select the device of interest and then try to use the Find Device tool to find it, whereas the latter directly opens the Find Device screen with the device of interest automatically selected so that all you need to do is to click the **Find** button to look for it.

Figure 8-1 shows the Find Device screen.

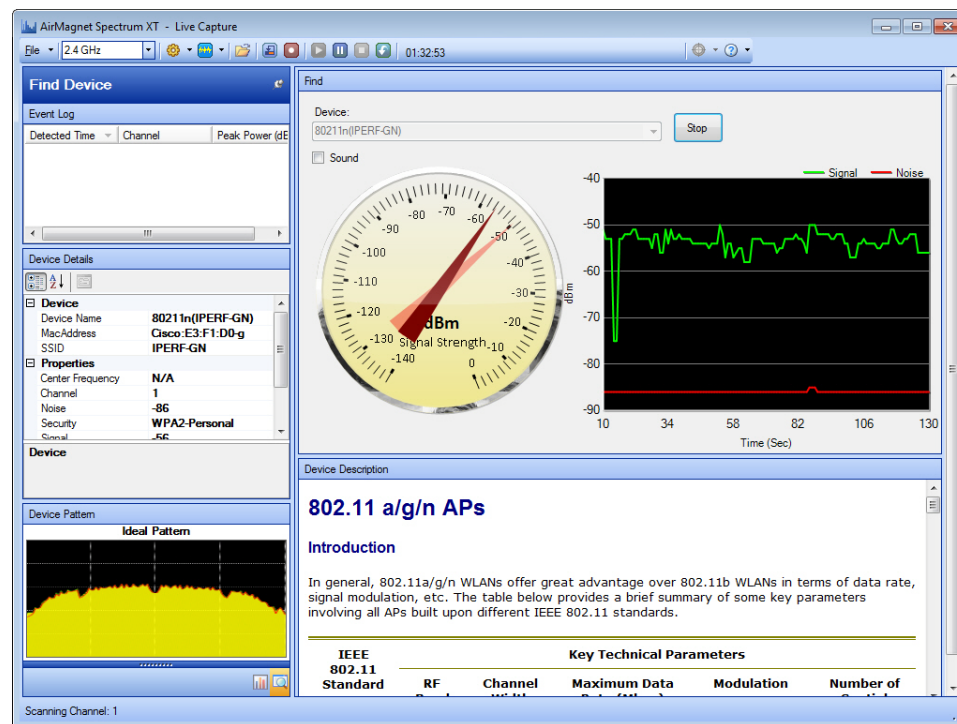


Figure 8-1: Find Device Screen

The following sections discuss in detail the various components of the Find Device screen.

Event Log

In the upper-left pane of the Find Device screen is the Event Log. It shows the following information about the device being selected:

- **Detected Time** - The data and time of each instance when the device was detected.
- **Channel** - The channel on which the device was detected.
- **Peak Power** - The maximum energy reading of the device at the time it was detected.

Device Details

The Device Details pane provides detailed information about the device being selected. See Figure 8-2.

Device Details	
Device Device Name 80211n(IPERF-GN) MacAddress Cisco:E3:F1:D0-g SSID IPERF-GN	
Properties Center Frequency N/A Channel 1 Noise -86 Security WPA2-Personal Signal -55	
Time First Seen Time 11/4/2009 8:48:15 AM Last Seen Time 11/4/2009 10:24:19 AM	
Device	

Figure 8-2: Detailed information about a selected device

The information displayed will vary, depending on the type of device detected (802.11 or non-802.11). As shown in Figure 8-2, the Device Details pane shows the following information for standard 802.11 devices:

- Device Name - The device category the selected device belongs to (i.e., Bluetooth Device, Digital Cordless Phone, etc.)
- Mac Address - The MAC address of the device.
- SSID - The SSID detected from the device.
- Center Frequency - The middle point of the frequency range detected for the device.
- Channel - The channel on which the device is operating.
- Noise - The level of noise detected from the device.
- Security - The security mechanism in use by the device.
- Signal - The signal level detected from the device (in dBm).
- First Seen Time - The first time the device was detected.
- Last Seen Time - The most recent time the device was detected.

For non-802.11 devices, the information differs:

- Device Name - The device category the selected device belongs to (i.e., Bluetooth Device, Digital Cordless Phone, etc.)
- Affected Channels - The range of channels being affected by the device.
- Average Power - The average energy reading of the device recorded since it was detected.
- Center Frequency - The middle point of the frequency range detected for the device.
- Peak Power - The maximum energy reading of the device since it was detected.

- First Seen Time - The first time the device was detected.
- Last Seen Time - The most recent time the device was detected.

Device Pattern

In the lower-left corner of the screen is the Device Pattern pane which shows the RF spectrum pattern of the device being selected. The is chart is also available on the Spectrum-WiFi Summary screen. See Figure 8-3.

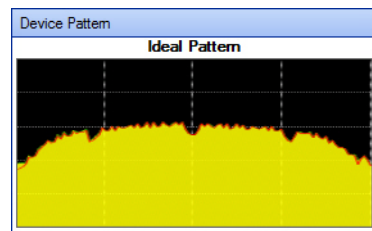


Figure 8-3: RF spectrum pattern of a selected device

As seen in Figure 8-3, the Device Pattern pane shows the spectrum pattern the application has detected of the selected device.

If the selected device is a WiFi device, the Device Pattern pane will show the Ideal Pattern only. If the selected device is a non-WiFi device, then it will show both the Ideal Pattern and the Detected Pattern. The application uses the Ideal Pattern as a reference when classifying devices it has detected and determines the type of device by matching the Detected Pattern with the Ideal Pattern. For example, if the application finds that a detected spectrum pattern matches that of the ideal spectrum pattern of a Bluetooth device, it will categorize the device as a Bluetooth device.

Note that the device pattern examples provided with AirMagnet Spectrum XT are intended to be baselines, not exact matches for the devices detected. The device pattern can vary even between two similar devices (i.e., two microwaves from different vendors). Consequently, the device's pattern may not always be an exact match for the example provided in the application.

Find Device Tool

The Find Device tool contains tools for locating any device (WiFi or non-WiFi) that has been detected on the network. See Figure 8-4.

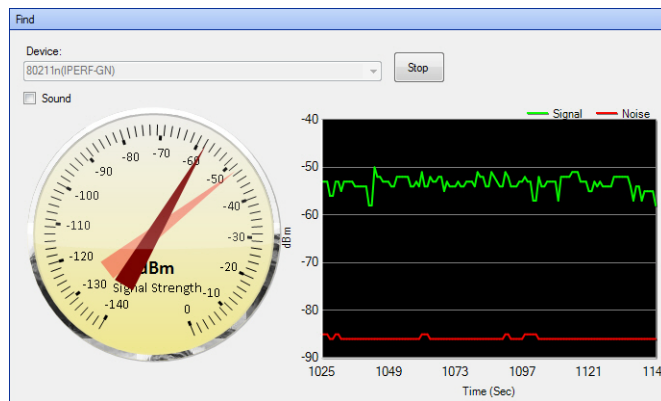


Figure 8-4: Close-up view of Find Device Tool

The Find Device tool has the following components:

- **Device Drop-Down List Menu** – Allows the user to select an entry among all detected devices in the selected radio band.
- **Find/Stop Button** – allows the user to start or stop a device-locating operation.
- **Sound Check Box** – If checked, the application will start ticking while searching for a device. The sound becomes louder as you get closer to the device.
- **Signal Strength Gauge** – Shows the change in signal strength as you move closer to the device. The lighter hand indicates the highest signal strength that has been recorded of the device and the darker one the signal strength reading of the device at the moment. Signal strength should become stronger as you move closer to the device you are intend to find.
- **Signal/Noise Graph** – Shows the changes in signal strength and/or noise level during a search operation. Both signal strength and noise level are graphed if the device you are trying to find is a WiFi device; only signal strength is shown if it is a non-WiFi device. Signal strength and noise level should rise as you move closer to the device you are trying to find.

Device Description

In the lower-right part is the Device Description pane, which contains detailed information about the (type of) device you are trying to find, which includes the following:

- 1) An brief introduction of the RF characteristics of the device, such as radio frequencies or channels, modulation, transmit rate, etc. of the device.
- 2) The typical RF spectrum pattern of the device.
- 3) Its impact on the WLAN.
- 4) Recommendations on how to minimize the device's interference on a WiFi network.

You can use the scroll bar or arrows on the right to view the full description of the device being selected.

Physically Locating a Device on the Network

Theoretically, you can locate any device that the application has detected on the network, using the following instructions.

To physically locate a device on the network:

- 1) Make sure that the device is selected in the Device Drop-Down List Menu.
- 2) Click Find.
- 3) Check the Sound check box, if you like.
- 4) Pick up your laptop PC and move in the direction the ticking sound gets louder and the signal strength get stronger until you finally reach the location of the device.

Best Practices

This section documents some recommendations for best results when attempting to locate devices using AirMagnet Spectrum XT.

With Omni-directional Antenna

- 1) Begin in the area where interference of the WiFi network has been reported.
- 2) On the Summary page, identify the non-WiFi device responsible for the interference on your network.
- 3) Go to the Find page.
- 4) From the drop down list, select the device you identified in Step 2.
- 5) Start the Find Tool.
- 6) Because the signal strength can greatly vary from second to second, begin a slow patrol of the area, covering a meter in 3 to 5 seconds.
- 7) When you reach an area where the signal has climbed to its highest level, look around to locate the device.

With Directional Antenna

- 1) Begin in the area where interference of the WiFi network has been reported.
- 2) On the Summary page, identify the non-WiFi device responsible for the interference on your network.
- 3) Go to the Find page.
- 4) From the drop down list, select the device you identified in Step 2.

- 5) Start the Find Tool.
- 6) Slowly turn around until you locate the direction in which the device's signal strength is the strongest.
- 7) As directly as possible, move in the direction of the strongest signal. Move slowly, covering about one meter every three to five seconds.
- 8) When the signal has climbed to its highest point, or appears to be roughly the same no matter what direction the antenna is facing, observe the area to locate your interfering device.

Chapter 9: Radar Detection Tool

Chapter Summary

This chapter discusses the Radar Detection Tool that can be used to detect radar in the wireless LAN environment. It covers the following topics:

- Introduction
- Radar Tool UI Components
- Using the Radar Detection Tool

Introduction

The 5-GHz band is an Unlicensed National Information Infrastructure (UNII) band, which is divided into several segments, each being designated for a specific use. The UNII-2 (5.25 GHz~5.35 GHz) and UNII-2 extended (5.47 GHz~5.725 GHz) bands used to be set aside exclusively for military and weather radar systems. When the FCC decided to open these bands up for WiFi networks, its ruling came with an important caveat: Dynamic Frequency Selection version 2, or DFS2, compliance.

DFS is a mechanism that tells the transmitter to dynamically listen for radar signals in the airwave and automatically switch to another channel if a radar signal is detected. The mechanism is designed to protect the incumbent military and weather radar systems from the RF interference from 802.11a/n devices in their vicinity. With DFS2, the transmitter on a WiFi device will continuously listen for radar signals, both before and during transmission. If a radar signal is detected on a channel, it will either vacate that channel or flag it as unavailable.

DFS2 is a must-have on 802.11a/n APs in order for 802.11a/n network systems to co-exist with military and weather radar systems. According to the latest FCC ruling, all WiFi devices operating in the UNII-2 and UNII-2 extended bands are required to support DFS, to detect and automatically switch channels to prevent WLAN operations from interfering with military or weather radar systems. The mandate became effective on July 20, 2007 in the US and Canada. A similar mandate became effective on April 1, 2008 in the EU.

Since then, in April 2009 new EN 301 893 v1.5.1 requirements also called DFS-3 Compliance have also been enforced for 802.11 APs operating in Europe.

AirMagnet Spectrum XT Radar Detection Tool

The only radar signals that AirMagnet Spectrum XT can detect are those described by the regulatory bodies as part of the DFS requirements.

AirMagnet Spectrum XT supports all six of the FCC radar types, all six of the ETSI EN 301 893 V1.5.1 radar types, and all eight of the ETSI EN 302 502 V1.2.1 radar types.

Of the ten radar types defined by the Japanese DFS requirements, AirMagnet Spectrum XT supports Type 1, and Types 5-10, which have exact equivalents in the FCC types.

Japanese radar Types 2-4 are currently not supported.

Note: Most radar signals come in short bursts, followed by a dead time. Detection by SpectrumXT would require that the bursts arrive while the SpectrumXT is on the correct channel. The chances of this happening in the short-term may be very low. The best way to detect the radar is to dwell on each channel for a period of time that includes several sweeps of the radar. This could range from 10ths of seconds to several minutes.

Impact on 802.11 WLAN

Since the 802.11a/n wireless network shares the same radio frequency bands/channels with military and weather radar systems, the FCC regulation and requirements on DFS/DFS2/DFS3 undoubtedly puts some serious challenge to the operation of the 802.11a/n wireless network. Care must be taken to ensure that WLAN operation will not interfere with or disrupt the normal operation of radar systems.

Recommended Courses of Action

Based on FCC regulations, the following actions are recommended on the part of the 802.11a/n wireless network in order to minimize or eliminate its potential interference with military and/or weather radar systems:

- Make sure all 802.11a/n devices that are operating on your WLAN are DFS2 or 3-certified.
- If you have uncertified 802.11a/n devices on your network, make sure that the UNII-2 and UNII-3 bands/channels are blocked.

If you have 802.11a/n devices that are manufactured prior to July 20, 2007 (US), then check with the vendors for possible firmware upgrade. The same goes for DFS3 requirements in Europe.

Radar Detection Tool UI Components

This section describes the options in the Radar Detection Tool user interface.

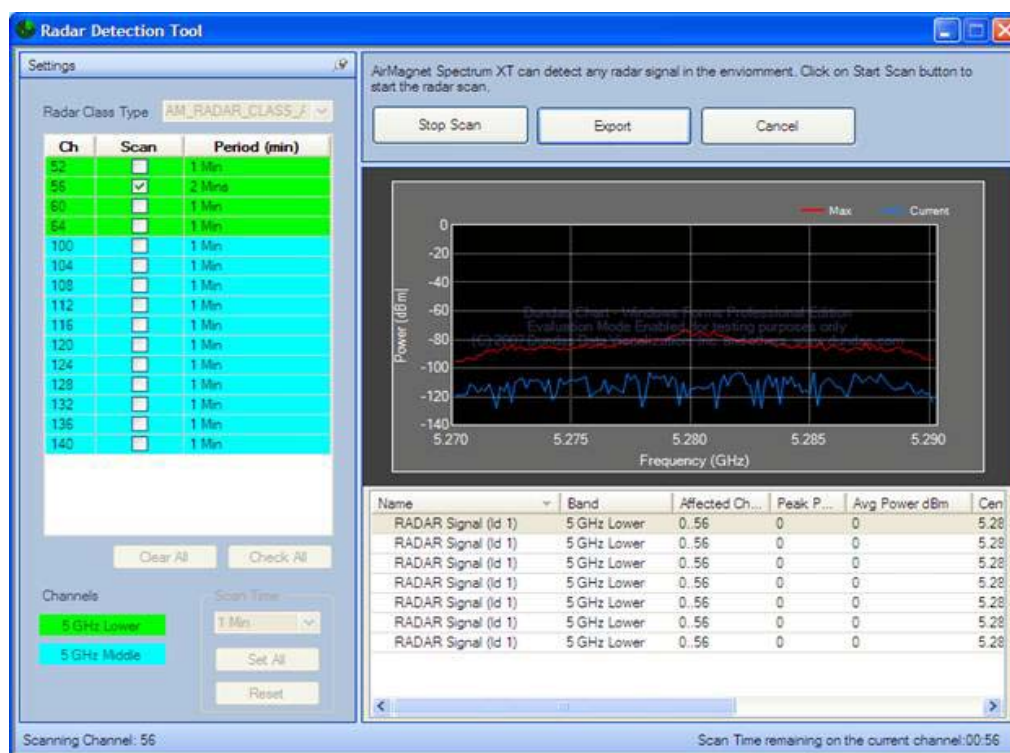


Figure 9-1: Radar Detection Tool User Interface

Table 9-1: Radar Detection Tool UI Components

Option	Description
Settings bar	This is the heading for the Settings panel. You may collapse the Setting panel by clicking the push pin icon located to the right of the Settings bar. Once collapsed, to view the panel, click the Settings tab in the top left corner. To re-establish the default view, click the push pin.
Radar Class Type	FCC: Federal Communications Commision channels for United States. ETSI: European Telecommunications Standards Institute channels for Europe. TELEC: Telecommunications Engineering Center channels for Japan.
Ch (Channel)	This column lists the channels for the selected Radar Class Type

Table 9-1: Radar Detection Tool UI Components

Option	Description
Scan	When the box next to a channel listing is checked, this channel will be scanned during a scanning session.
Period (min)	This column provides a drop-down menu for each channel that can be used to manually set the time the associated channel will be scanned during the session.
Clear All	Click this button to un-check all the channels.
Check All	Click this button check all the channels
Reset	Click this button to check all the channels and reset the “Period” column to the default setting of 1 min.
Band	This is a color legend that indicates the media type for the channel listing.
Scan Time	Using this option will automatically set all the channels to the period set using the drop-down.
Start Scan	Click this button to begin a radar scanning session.
Stop Scan	Click this button to end a radar scanning session.
Export	Select a radar device listing and click Export to export the data in .csv format.
Cancel	Click this button at any time to cancel a scanning session and close the Radar Detection Tool window.
Radar Graph	During an active scanning session, the radar graph charts real-time data by plotting a function of the frequency range and the power in dBm for the current channel being scanned
Radar Device Table	The table below the graph will list any radar devices detected during the scanning session. Name: The device signature detected. Band: The UNII band the device was detected in. Peak Power dBm: The highest power level detected for the device. Avg Power dBm: The average power level detected for the device for the scanning period. Center Frequency GHz: Refers to the center frequency of the device. Affected Channel: The channel that is affected by the device. First Seen Time: When the device was detected for the first time. Last Seen Time: The most recent time when the device was detected.
Status bar	Scanning Channel: During a scanning session, the current channel being scanned will be displayed in the lower left side of the status bar. Scan Time: During a scanning session, the time remaining for the scan of the current channel will be displayed in the lower right side of the status bar. The format is min min: sec sec.

Using the Radar Detection Tool

To use the Radar Detection Tool:

- 1) From the **File** menu select **Radar Detection Tool**. This will open the Radar Detection Tool window.
- 2) In the **Settings** panel, select the desired Radar Class Type from the drop-down menu.
- 3) Set the desired channels to scan by adjusting the checked options in the **Scan** column.
- 4) Set the scan period for each channel by adjusting either each channel individually by using the **Period** column drop-down for each channel (See [Figure 9-2](#)) – or – set the scan time for all checked channels using the **Scan Time** drop-down menu. To use **Scan Time**, select a time from the drop-down and click **Set All**.

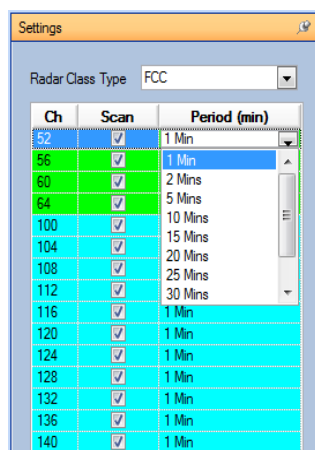


Figure 9-2: Period (min) drop-down menu

- 5) Click **Start Scan** to begin the channel scanning session.

The graph will begin to chart the power and frequency data for the channel being scanned. The channel being scanned will be listed at the bottom left of the window in the status bar. If radar is detected, the device detected will be listed in the table below the graph.

- 6) Click **Stop Scan** to end the session.
- 7) If at least one radar device is listed in the table below the graph, the listing data may be exported in .csv format. To do this, select the listing and click **Export**. Browse to a folder location to store the data file.

*Note: The Radar Detection Tool may be closed at any time by clicking **Cancel**.*

Chapter10: Device Detection

Chapter Summary

AirMagnet Spectrum XT can detect and identify various 802.11 or non-802.11 devices that are operating in your WiFi network by looking at the unique patterns of energy emitted from those devices. This chapter discusses the major categories of devices that AirMagnet Spectrum XT is able to detect. It talks about the modulation method, typical RF spectrum pattern, impact on WiFi networks of these devices. It also offers recommendations on how to minimize or eliminate the RF interference to the WiFi network caused by these devices.

AirMagnet Spectrum XT has the capability to detect and identify the following non-WiFi devices based on their unique RF spectrum patterns:

- Bluetooth Devices
- Digital Cordless Phones
- Analog Cordless Phones
- Microwave Ovens
- Baby Monitors
- Wireless Cameras
- Digital Video Monitors
- Zigbee
- Wireless Mouse
- Motion Detector
- RF and Narrowband Jammers
- RF Signal Generator
- Non-Bluetooth Wireless Mouse
- Wireless Game Controllers
- Frequency Hopping Spread Spectrum devices

AirMagnet Spectrum XT is also able to detect all WiFi devices and identify their RF spectrum patterns of 802.11 APs:

- 802.11a/g/n APs
- 802.11b APs

Note that the device pattern examples provided with AirMagnet Spectrum XT are intended to be baselines, not exact matches for the devices detected. The device pattern can vary even between two

similar devices (i.e., two microwaves from different vendors). Consequently, the device's pattern may not always be an exact match for the example provided in the application.

Non-WiFi (Spectrum) Devices

The section discusses the various non-WiFi (spectrum) devices that AirMagnet Spectrum XT is able to detect in a wireless network environment. It talks about their typical RF spectrum patterns, impact on WiFi networks, and the best ways to minimize their interference to the 802.11 network.

Bluetooth Devices

Like most cordless phones on the market today, Bluetooth device also operate in the same 2.4-GHz radio band used by 802.11b and 802.11g wireless LANs (WLANs). The problem is that Bluetooth devices and 802.11b/g WLANs are based on two different modulation technologies, which make their radio signals behave so differently that it is difficult for them to operate in the same band without interfering with each other. Bluetooth devices, on the one hand, are based on Frequency Hopping Spread Spectrum (FHSS) modulation. Their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. 802.11b/g WLANs, on the other hand, use Direct Sequence Spread Spectrum (DSSS) modulation technology that allocates only three 22-MHz wide bands within the 2.4-GHz spectrum and transmits over only one of those bands at any given time. Because radio signals from Bluetooth devices hop across all channels randomly across the entire 2.4-GHz radio band, they have a detrimental effect on 802.11b/g WLANs that operate in the same 2.4-GHz band. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, i.e., channels 1, 6, and 11), it is hard for 802.11b/g APs to escape the RF interference caused by Bluetooth devices operating on or in the vicinity of your network. Bluetooth devices can cause performance degradation when used in close proximity to 802.11 stations, especially when the latter are relatively far away from the APs or stations they are associating with, because of weak signal strength.

RF Spectrum Pattern

Figure 10-1 shows the RF spectrum pattern of a Bluetooth-enabled iPhone.

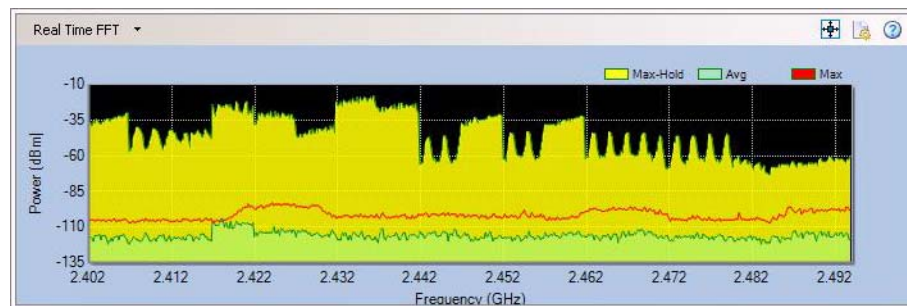


Figure 10-1: RF spectrum pattern of a Bluetooth-enabled iPhone

Impact on 802.11b/g WLAN

Because the 2.4-GHz radio band is unlicensed (free to all), there are numerous Bluetooth-enabled devices by different manufacturers available on the market. The following is a short list of such devices:

- Laptops
- PDAs
- Headsets
- Headphones
- Mice
- Keyboards
- Dongles
- Adapters
- Speakers, etc.

These Bluetooth devices are becoming increasingly popular in homes and businesses where 802.11b/g WLANs are deployed and have been recognized as a source of RF interference to 802.11b/g WLANs. You may tackle these interfering Bluetooth devices by identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering Bluetooth devices are successfully located, the following actions are recommended to minimize or eliminate the RF interference they cause to your 802.11b/g WLAN:

- Change your WLAN from 802.11b/g to 802.11a or upgrade it to 802.11n standard and set it up to run in the 5-GHz channels or frequencies, which will not only avoid RF interference from Bluetooth devices operating in the crowded 2.4-GHz band but also offer greater throughput.
- Try to use Bluetooth devices that are based upon Bluetooth specification version 1.2 or later which uses Adaptive Frequency Hopping (AFH) which limit the use of pseudorandom frequencies by Bluetooth devices when interference is detected. It helps prevent Bluetooth devices from interfering with other transmissions in the 2.4-GHz band.

Digital Cordless Phones

Most digital cordless phones on the market today operate in either the 2.4-GHz or 5.8-GHz radio band, which happen to be the channel or frequencies used by 802.11b/g or 802.11a wireless LANs (WLANs). The problem is that the two are completely different systems that do not understand each other. As a result, radio signals from the two different systems will collide and cause mutual RF interference. This is especially the case when 2.4-GHz FHSS digital cordless phones are involved. Because they use FHSS modulation, their radio signals hop from one frequency to another across the entire 2.4-GHz band, in searching for the best channel or frequency to use. This hopping behavior will cause persistent RF interference to the

802.11b/g WLAN in close proximity. As a result, no matter which channel your WLAN use or switch to (Remember that there are only 3 non-overlapping channels in the 2.4-GHz radio band, i.e., channels 1, 6, and 11), it is hard for 802.11b/g APs to escape the RF interference caused by 2.4-GHz FHSS digital cordless phones. Such sources of interference can cause significant disruption in WLAN service and performance degradation.

RF Spectrum Pattern

There are numerous digital cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

Below is a short list of digital cordless phones:

- Panasonic KX-TGA271 (2.4-GHz, FHSS)
- Panasonic KX-TG2700S (2.4-GHz, FHSS/DSS)
- Panasonic KX-TG5050 (5.8-GHz, DSS)
- AT&T 2355 (2.4-GHz)
- AT&T E5965C (5.8-GHz, FHSS/DSS. *The base transmits in 5.8 GHz whereas the phone transmits in 2.4 GHz.*)
- Uniden EX15660 (5.8-GHz)

Figure 10-2 and Figure 10-3 show the RF spectrum patterns of a 2.4-GHz and a 5-GHz digital cordless phone, respectively.

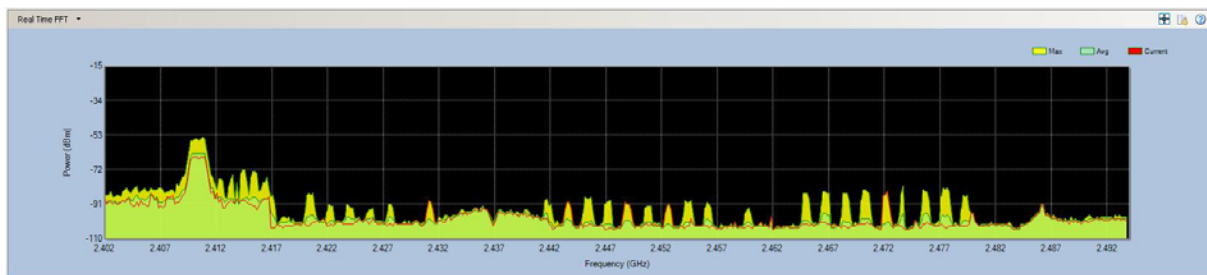


Figure 10-2: RF spectrum pattern of a 2.4-GHz DSSS digital cordless phone

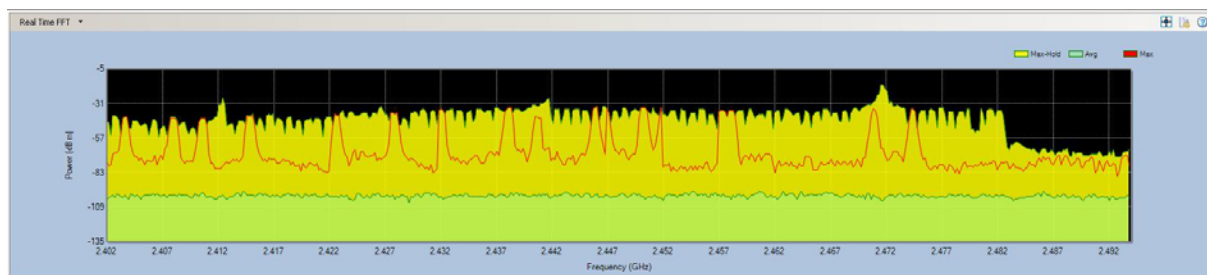


Figure 10-3: RF spectrum pattern of a 2.4-GHz FHSS digital cordless phone

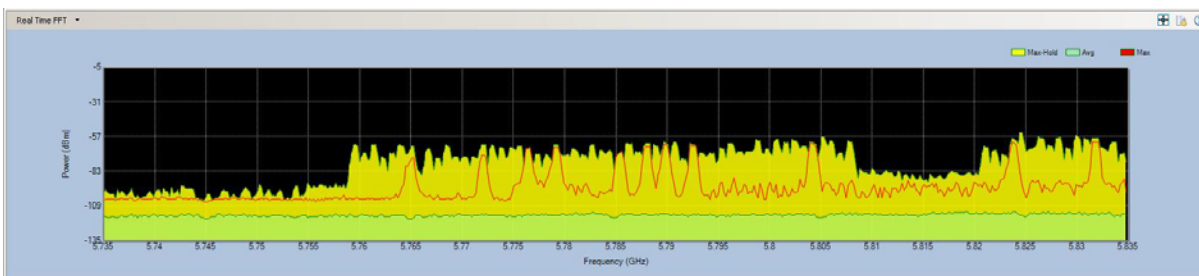


Figure 10-4: RF spectrum pattern of a 5.8-GHz FHSS digital cordless phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz digital cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11b/g or 802.11a WLANs are deployed. They have been recognized as a major source of RF interference for 802.11b/g or 802.11a WLANs. You may tackle these interfering 2.4-/5-GHz cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11b/g or 802.11a WLAN:

- Do not waste your time switching AP channels, because RF signals from digital cordless phones spread over all channels or frequencies in the band they operate. Simply adjusting AP channel is not the solution.
- If you have an 802.11b/g WLAN, avoid or stop using 2.4-GHz FHSS cordless phones. Instead replace them with 5.8-GHz or even old 900-MHz cordless phones which use different radio bands and channels.
- If you have an 802.11a WLAN, avoid or stop using 5-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g WLAN and 2.4-GHz cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5-GHz cordless phones along with 802.11b/g or 802.11a WLANs but try to maximize the distance between APs and cordless phone bases to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Analog Cordless Phones

Analog cordless phones are another source of interference to 802.11b/g or 802.11a wireless LANs (WLANs). Unlike digital cordless phones, analog cordless phones use narrowband transmission which occupies only a narrow bandwidth of the RF spectrum. Because of this, they can cause severe interference to an 802.11a/b/g AP operating in the same channel or frequency even though no significant interference to APs on other non-overlapping channels has been noticed.

One lab study found that an analog cordless phone transmitting on 2.412-GHz frequency which happens to be the center frequency of Channel 1 of the 802.11b/g WLAN can effectively take out the wireless connection on that channel the moment the phone which is placed next to an AP is turned on, whereas connections on the other two non-overlapping channels (6 and 11) were barely affected. The study also found that network throughput could drop by 99% with the analog cordless phone placed at 50 feet away from the AP, 20% at 100 feet away, and 5% at 150 feet away. The study concluded that analog cordless phones, if placed close to APs, can virtually disrupt wireless connection on the channel they operate.

RF Spectrum Pattern

There are numerous analog cordless phones available on the market today. They are widely used in homes and businesses and are also a source of RF interference to the 802.11 WLAN.

Below is a short list of analog cordless phones:

- GE 27923GE (2.4-GHz)
- Uniden EXP4540 (2.4-GHz)

Figure 10-5 shows the RF spectrum pattern of a 2.4-GHz analog cordless phone.

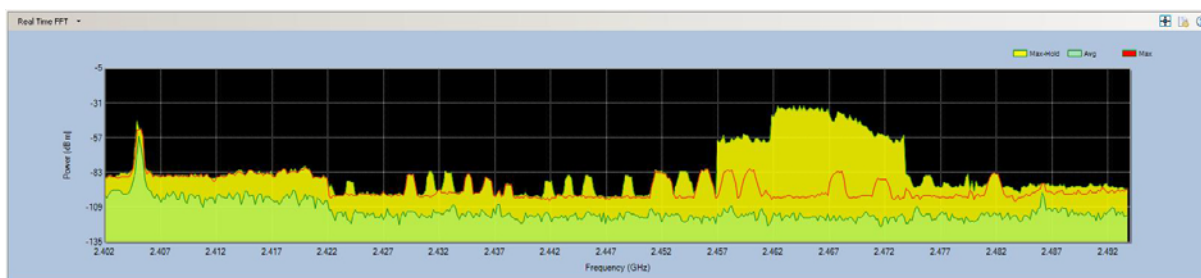


Figure 10-5: RF spectrum pattern of a 2.4-GHz analog cordless phone

Impact on 802.11 WLAN

Because the 2.4-GHz and 5-GHz radio bands are unlicensed (free to all), there are numerous 2.4-/5-GHz analog cordless phones by different manufacturers available on the market. They are widely used in homes and businesses where 802.11b/g or 802.11a WLANs are deployed. They have been recognized as a major source of RF interference for 802.11b/g or 802.11a WLANs. You may tackle these interfering 2.4-/5-GHz analog cordless phones by first identifying and locating them in your WLAN.

Recommended Courses of Action

Once interfering analog cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11 WLAN:

- If you have an 802.11b/g WLAN, avoid or stop using analog cordless phones on the same channel as your 802.11a/b/g APs. Instead try to set them on other non-overlapping channels.
- If you are using an 802.11b/g WLAN, try to use 5.8-GHz or even old 900-MHz analog cordless phones which use different radio bands and channels.
- If you have an 802.11a WLAN, avoid or stop using 5.8-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g WLAN and 2.4-GHz analog cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.
- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5.8-GHz cordless phones along with 802.11b/g or 802.11a WLANs but try to maximize the distance between WLAN APs and cordless phone bases to minimize RF interference between or among them.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

Microwave Ovens

Most microwave ovens used in homes and businesses today operate in the 2.45-GHz frequency, which is roughly the frequency of Channel 9 in an 802.11b/g WLAN. When a microwave oven is operating, the radio waves emitted from the radio antenna inside the oven are mostly confined within the oven's case, with only a small amount leaking out sometimes, especially with old ovens. To an 802.11b/g WLAN operating within close proximity, the radio waves that leak out of the microwave oven are a source of RF interference that may cause serious performance issues. This is because the interfering radio signals leaking out of the microwave oven will cause WiFi station to hold off transmission until the airwave is clear, causing network delay in the process. Furthermore, interfering RF signals do not follow the rules of the 802.11 protocols and are rather unpredictable: they can come and go at any time, disrupting normal communications between 802.11 devices in the WLAN. Study found that a microwave oven operating within ten feet of an 802.11b/g access point (AP) could cause a 75% drop in network throughput on Channel 9 (2.45 GHz frequency). Significant drop in throughput was also observed on adjacent channels such as Channels 8, 10, and 11. The impact was more severe near the edges of the AP's coverage area.

RF Spectrum Pattern

Figure 10-6 shows the RF spectrum pattern of radio signal from a microwave oven.

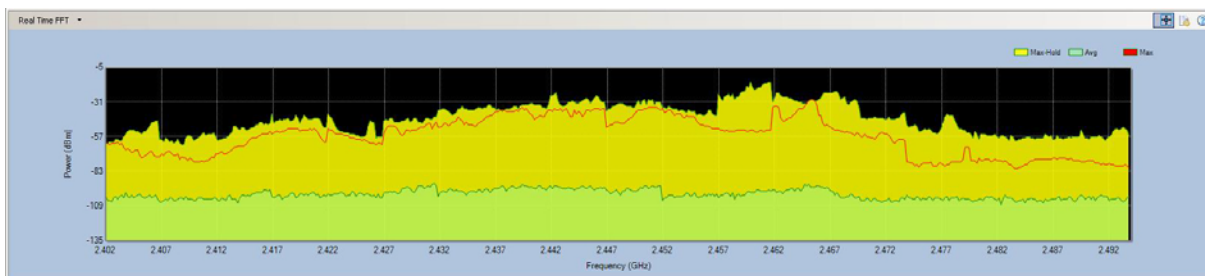


Figure 10-6: RF spectrum pattern of a microwave oven

Impact on 802.11b/g WLAN

Because microwave ovens are widely used in homes and businesses where WLANs are deployed, radio signals leaking out of an operating microwave oven have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down basic Internet applications such as Web file download and surfing. In the worst cases, they can knock out the network connection completely.

Recommended Courses of Action

Once the interfering microwave oven is successfully located, the following actions are recommended to minimize or eliminate the RF interference it causes to the 802.11 WLAN:

- Avoid using 802.11b/g WLAN near a microwave oven.
- When actively using WLAN applications (e.g., downloading files, video-conferencing, searching the Internet), make sure to keep a “safe” distance (at least 10 feet away) from an operating microwave oven. The farther away you are from the microwave oven, the less the interference.
- Find out the center frequency (which may vary depending on make, brand, or model) of a microwave oven from its label, and try to steer your WLAN away from it.
- Change your 802.11b/g WLAN to 802.11a or upgrade it to 802.11n, which will not only avoid RF interference from microwave ovens operating in the crowded 2.4-GHz band but also offer greater throughput.

Wireless Cameras

A wireless security camera is typically made up of three components: a camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a monitor or a recording device.

Most wireless cameras operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, wireless security cameras installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a wireless security camera can travel a relatively long range

which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, wireless security cameras installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Wireless cameras come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, etc. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.

Figure 10-7 shows the RF spectrum pattern of a wireless security camera.

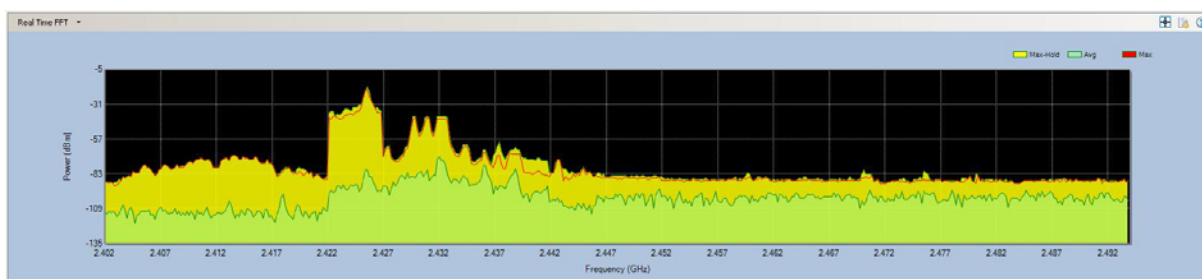


Figure 10-7: RF spectrum pattern of a wireless security camera

Impact on 802.11b/g WLAN

Because wireless cameras are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g WLAN, avoid using 2.4-GHz wireless cameras. Instead, use 5.8-GHz wireless cameras that operate in the licensed, less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11n standard which offers better interference avoidance.
- If you are using an 802.11a WLAN, avoid using 5.8-GHz wireless cameras.
- Check the operating channels on the wireless cameras, making sure that they do not overlap with the operating channels of the WiFi network.

Baby Monitors

Wireless baby monitors (digital or analog) use radio frequencies to transmit their signals. These same radio frequencies are also used by wireless networks installed in the home environment. As a result, RF interference will occur when the two competing systems are operating in the same radio frequencies.

RF Spectrum Pattern

Most wireless baby monitors on the market today use the 2.4-GHz frequency, a bandwidth also used by the 802.11b/g wireless network and many other wireless devices. The figure below shows the RF spectrum pattern of an analog baby monitor in the 2.4-GHz frequency band.

Figure 10-8 shows the RF spectrum pattern of a baby monitor

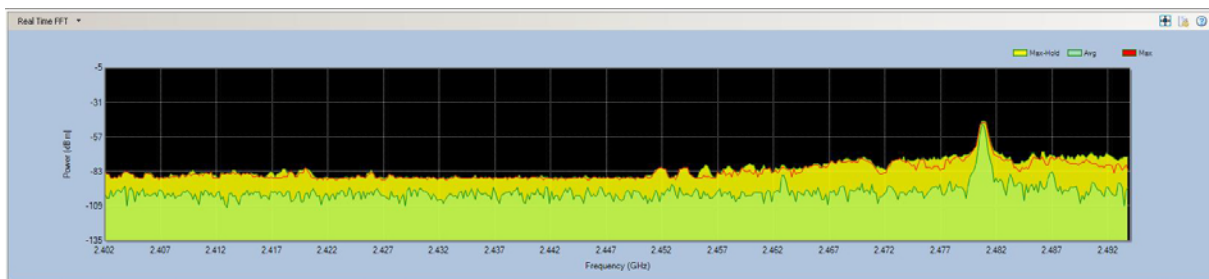


Figure 10-8: RF spectrum pattern of a baby monitor

AirMagnet Spectrum XT will detect FHSS, DSSS and Single Carrier models of baby monitors.

Impact on WiFi Networks

Generally speaking, RF interference is not an issue when a baby monitor is not in use. However, when it is in operation, it could have a negative impact on an 802.11 network, especially when they are in close proximity. When the baby monitor is turned on, the device will compete for bandwidth with the wireless network that is using the same radio frequency, causing the wireless network to experience performance degradation as a result of RF interference, and vice versa. The impact is more obvious for web applications involving downloading files over the Internet or Voice over IP. The figure below shows the RF spectrum pattern of a wireless analog baby monitor using the 2.4-GHz frequency band.

Recommended Courses of Action

Once an interfering wireless baby monitor is successfully identified, you can take all or some of the following actions to minimize or eliminate the RF interference it causes to your 802.11 WLAN.

- Check the channels or frequencies used by your wireless network and wireless baby monitor to make sure that they are not competing on the same channel or frequency.
- Since most of the wireless baby monitors today operate in the 2.4-GHz frequency band, try to upgrade your wireless network to the 802.11n standard.

- If you do not want to upgrade your wireless network, then try to get a wireless baby monitor that uses any radio frequency other than 2.4 GHz, such as 900 MHz.
- Since a baby monitor does not severely disrupt a wireless network unless the two are installed close together, try to place the wireless baby monitor and the wireless router as far apart as possible.

RF and Narrowband Jammer

RF Jammer is designed to block WiFi/WLAN/Bluetooth networks which work on the 2.4-GHz frequency band. It could help you cut off WiFi connections in targeted areas of a WLAN and prevent leaking out sensitive data.

Narrowband Jammer is designed to block Wi-Fi/WLAN/Bluetooth networks for a specific area of the screen on a 2.4GHz frequency. It could help to cut off WiFi connections in targeted areas of a WLAN and prevent leaking out sensitive data. See [Figure 10-9](#).

RF Spectrum Pattern

RF Jammers operate in the 2.410~2.480 GHz frequency range. Their radio signals can transmit in a 15 feet radius with output power of 7 dB.

[Figure 10-9](#) shows the RF spectrum pattern of an RF Jammer.

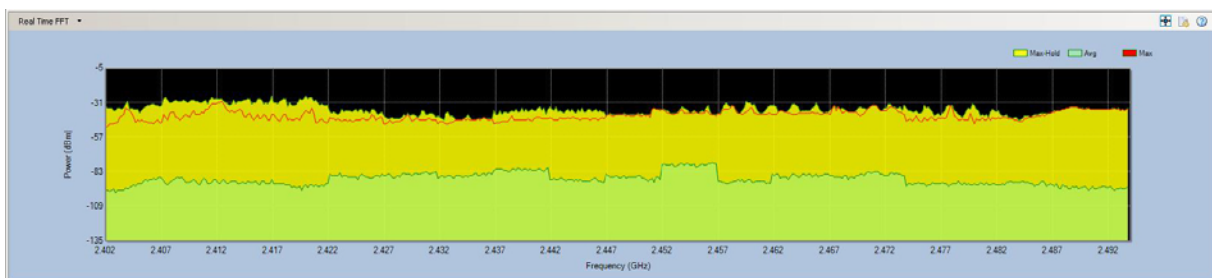


Figure 10-9: RF spectrum pattern of an RF Jammer

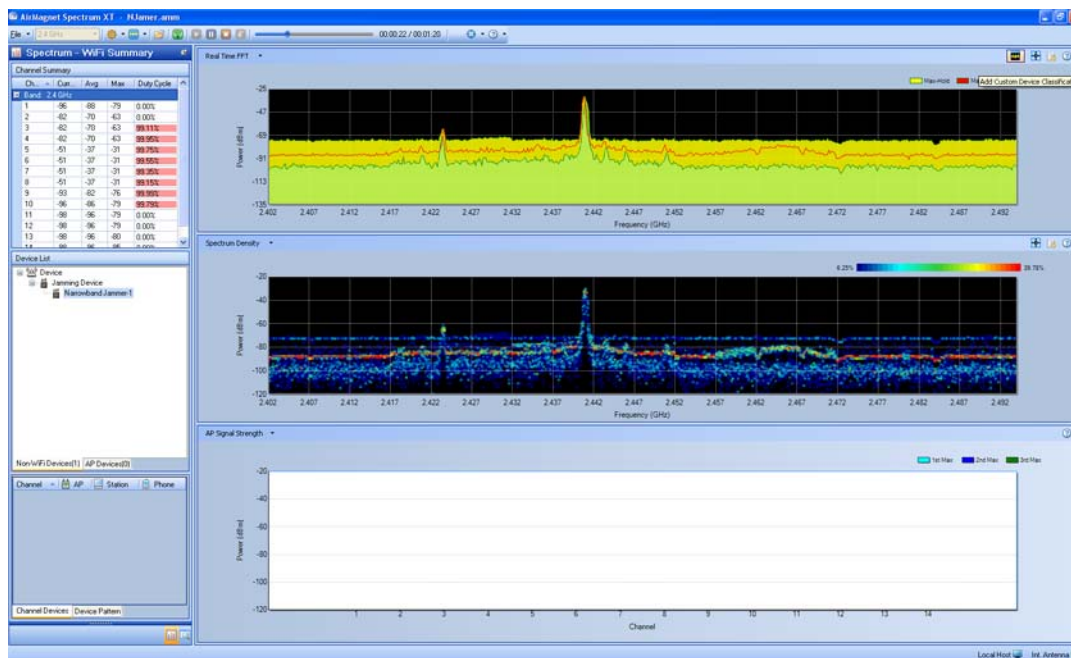


Figure 10-10: Interference Source - Narrowband Jammer

Impact on WiFi on WiFi Networks

WiFi Jammers are designed to protect important working area and avoid leakage of sensitive data by blocking WiFi networks. Since it works in the 2.4 GHz frequency band and channels, this type of device can be a good “defensive” tools against data leakage over wireless network, but can also be a “double-edged sword”. Anyone could use it to disrupt the operation of a wireless network. Because of its compact design, it can be hidden in a pocket or briefcase or elsewhere and can be carried around and deployed at any location of a network without being discovered.

Recommended Course of Actions

Since RF Jammers operate in the same 2.4-GHz frequency band as 802.11b/g networks do, the following actions are recommended in order to minimize or eliminate their interference to 802.11b/g WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF Jamter is causing interference to your WLAN.
- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Jammers, if they are necessary.

Digital Video Monitors

A digital video monitor is typically made up of three components: a video camera, a transmitter to send the signal, and a receiver to receive the signal. The system works in such a way that the wireless camera transmits video from the built-in transmitter to the receiver, which is connected to a display device (monitor) or a recording device.

Most digital video monitors operate on the 2.4-GHz frequency – an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, digital video monitor installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation of the WLAN. Unlike the other RF interfering devices operating in the 2.4-GHz band, radio signals from the transmitter of a digital video monitor can travel a relatively long range which varies from 200 to 700 feet (line of sight), depending on the physical conditions of the site. Typically, multiple cameras are needed in order to provide full, overlapping coverage of one site. To make matters worse, digital video monitors installed in homes and businesses are left on all the time. And so is the RF interference they cause to the 802.11 WLAN close to them.

RF Spectrum Pattern

Digital video monitors come in all shapes and sizes. They include wireless surveillance cameras, spy cameras, etc. They are widely used in homes and businesses where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless camera using the 2.4-GHz frequency band.

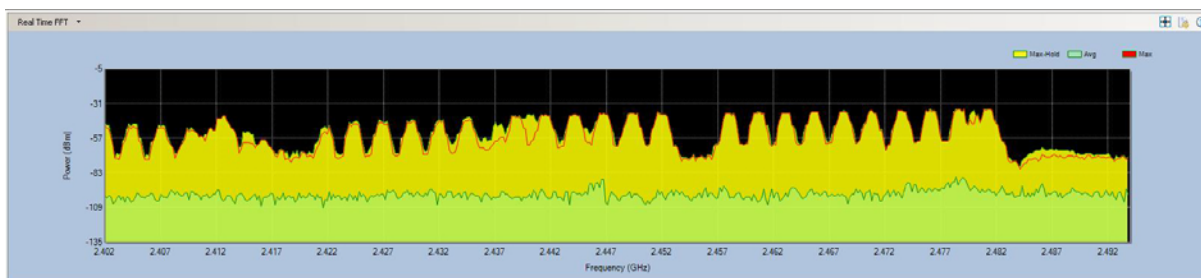


Figure 10-11: RF spectrum pattern of a digital video monitor

Impact on 802.11b/g WLAN

Because digital video monitors are widely used in homes and businesses where WLANs are deployed, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in these settings. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless security cameras are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- If you are using an 802.11b/g WLAN, avoid using 2.4-GHz digital video monitors. Instead, use 5.8-GHz video monitors that operate in the less crowded 5-GHz radio band. Or upgrade your WLAN to the 802.11n standard which offers better interference avoidance.
- If you are using an 802.11a WLAN, avoid using 5.8-GHz digital video monitors.
- Check the operating channels on the digital video monitors, making sure that they do not overlap with the operating channels of the WiFi network.

Zigbee

A low-cost, low-power, and short-range wireless mesh networking standard based on the IEEE 802.15.4 specifications. Zigbee devices can operate in the 860-MHz, 915-MHz, or 2.4-GHz band using DSSS modulation. First ratified in 2005, billions of dollars has been invested in Zigbee technology and Zigbee-based devices have now found their way into homes and businesses. Typical applications include:

- Home Entertainment and Control - Audio/video systems, smart lighting, temperature control
- Safety and Security Monitoring - Sensors (access, water, and power), smoke detectors, smart appliances
- Commercial Property Management - Access control, lighting, energy monitoring, HVAC
- Industrial Automation - Process and device control, asset/energy/environmental management.

RF Spectrum Pattern

For network administrators, it is the 2.4-GHz Zigbee devices that cause concern because they use the same radio frequencies as the 802.11b/g wireless networks do. 2.4-GHz Zigbee devices can operate on one of 16 non-overlapping channels (11 in North America) that are 3 MHz wide and 5 MHz apart. Generally, a Zigbee mesh network uses only one channel. Once set up, it stays on that channel until it is changed manually. Zigbee radios use very low transmit power (typically -3dBm or 0.5mW) and receive sensitivity (between -80dBm and -100dBm depending on radio.) Their maximum bit transfer rate is 250 Kbps. Even though the size and length of Zigbee data packets vary, their target applications are of low duty cycle and low power consumption. Because of this, the Zigbee network does not have as much traffic in comparison to an 802.11b/g network.

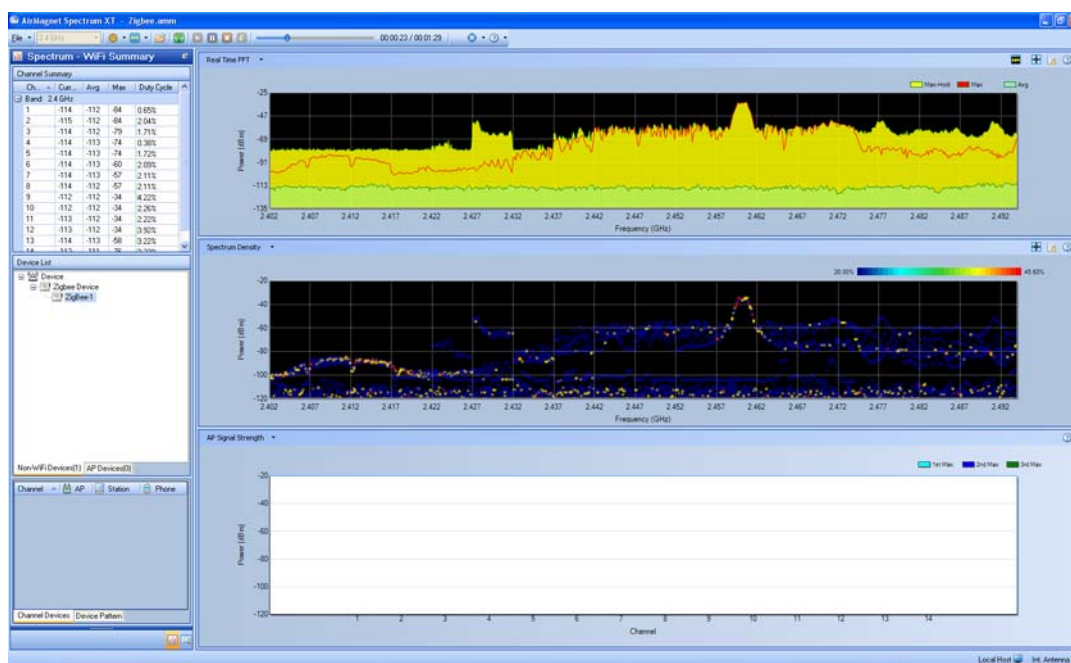


Figure 10-12: Interference Source - Zigbee

Impact on 802.11b/g WLAN

Given the fact that a 2.4-GHz Zigbee network operates on a fixed 3 MHz of bandwidth in the 2.4-GHz band, the chance of collision between a Zigbee device and an 802.11b or g device depends on the channels on which they operate. If the channels overlap, the chance are high. Otherwise, the chances are very low.

Recommended Courses of Action

Once a ZigBee network or devices are identified, the following actions are recommended to minimize or eliminate the potential RF interference that they may cause to the WiFi network:

- Try to set your ZigBee network to a non-overlapping channel not used by an 802.11b or g network.
- Try to keep ZigBee devices physically away from WiFi devices to minimize the chances of interaction.

Motion Detector

Motion detectors are devices that use a variety of methods to determine if a body of a significant size is moving through an area, usually as part of a security or energy management system. While most models use an infrared detection system, some newer models incorporate a microwave detection system. In some models, this microwave detection system transmits on a narrow band of frequency in the 2.4GHz band. While only active at times of motion detection, in areas of high pedestrian traffic, or areas of high WLAN traffic, these devices present the possibility of disrupting WLAN traffic if the transmitting frequency of the device corresponds with the channel the WLAN is operating on. AirMagnet Spectrum XT will detect S-Band radar based motion detectors that are operating in the environment.

RF Spectrum Pattern

Below is a sample of what the spectrum pattern for a motion detector would look like in a relatively noiseless 2.4GHz spectrum.

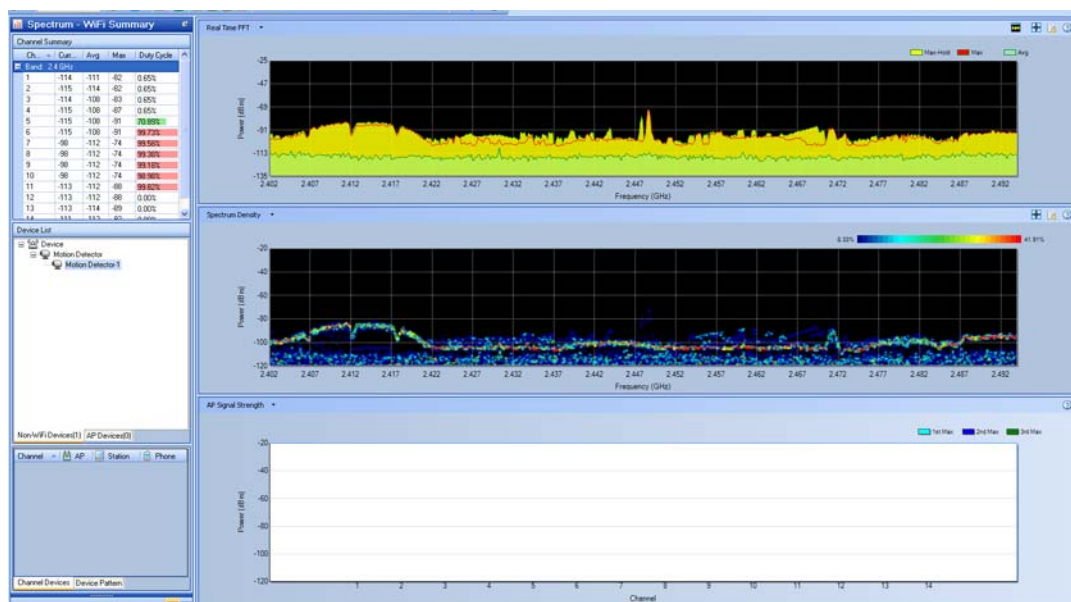


Figure 10-13: Interference Source - Motion Detector

Impact on 802.11 WLAN

The impact on 802.11 networks depends on the amount of pedestrian traffic near the motion detector.

- Because this technology only transmits a signal when the correct parameters for motion detection are met, in areas of low pedestrian traffic, the impact on a WLAN network will be low. The device may cause intermittent interference only if it is transmitting on a frequency

within the channel width of a WLAN AP, and only if it is significantly close enough to the WLAN network to have an impact.

- If the motion detector is in an area of high pedestrian traffic, is on a frequency within the channel width of the WLAN AP, and if it is significantly close enough to interfere with the WLAN, this device type can have a significant impact on a WLAN, behaving almost as a Narrow-band Jammer would.

Recommended Courses of Action

- If possible, change the channel that your WLAN is operating on to one that is unaffected by the Motion Detector.
- You may consider changing from the 2.4GHz band to one of the 5GHz bands, as these bands will not be affected by the Motion Detector.
- If you have to use your Motion Detectors along with 2.4GHz WLANs, try to maximize the distance between APs and Motion Detectors to minimize their RF interference.

RF Signal Generator

A device that generates repeating or non-repeating RF signals. An example of this type of device is the AirHORN Channel-Signal Generator. This USB PC-based product aids users in testing Wi-Fi antennas, RF shields and wireless networks. This RF Signal Generator covers the 2.4 and 5 GHz bands and generated RF signals for each Wi-Fi channels in those spectrums.

Recommended Courses of Action

AirHORN Channel-Signal Generator is a proprietary hardware/software solution sold by Nuts About Nets. Only the devices in this product category will show up as this device type.

Below is an example of what the spectrum pattern for what an AirHORN Channel-Signal Generator would look like in a relatively noiseless 2.4GHz spectrum.

Impact on 802.11 WLAN

Used incorrectly, the AirHORN Channel-Signal Generator can create a signal that will essentially block all WiFi and WLAN traffic across a 2.4 or 5 GHz ISM band, until it is either turned off or switched to a different channel.

Recommended Course of Action

Please follow the recommended actions to minimize or eliminate their interference to 802.11a/b/g/n WLANs:

- Monitor your WLAN on a regular basis to make sure that no RF signal generator is causing unintended interference to your WLAN.

- Conduct regular WLAN site RF surveys to determine the proper location and use of RF Signal Generators, if they are necessary.
- If it is necessary to use the RF Signal Generator, only use it on channels that do not overlap with the channels used by your WLAN.
- If optimal WLAN performance is not an issue, you may continue to use your RF Signal Generator along with your WLANs, and try to maximize the distance between APs and RF Signal Generator to minimize their RF interference.

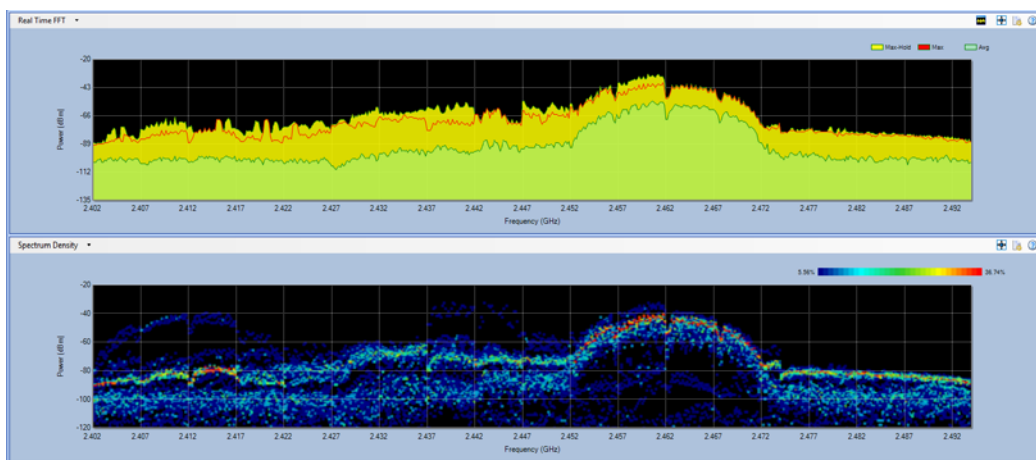


Figure 10-14: Interference Source - AiHorn Signal Generator

Non-Bluetooth Wireless Mouse

Since the 2.4 GHz and 5 GHz wireless spectrums are unregulated, companies are allowed to use those bands for more than just WLAN traffic. In response to some of the concerns about the interference between WLAN and Bluetooth networks, or between WLAN and continuous transmitter technologies like some cordless phones, some companies have developed

technologies that allow their devices to operate in a way that minimizes the impact on WLAN networks. With the ability to find a frequency with the least amount of WLAN traffic in the 2.4 GHz spectrum, non-bluetooth wireless mice minimize their impact on the WLAN network. See Figure 10-15 below.

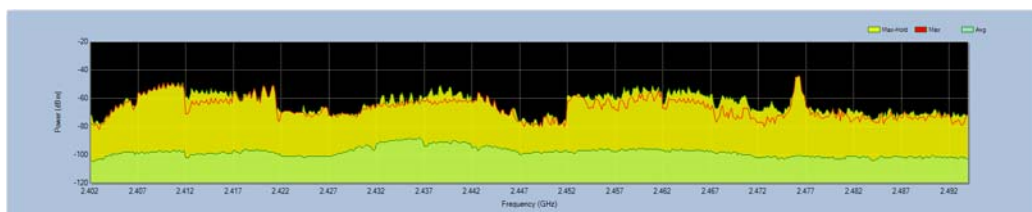


Figure 10-15: Non-Bluetooth Wireless Mouse Fill

RF Spectrum Pattern

To date, the only devices detected for this device type are made by Logitech. This is based on the new Logitech Advanced 2.4GHz wireless technology. The current models ship with this technology:

- Marathon Mouse M705
- Marathon Mouse M310
- Anywhere Mouse MX™
- Wireless Mouse M510
- Wireless Mouse M305
- Performance Mouse MX™
- Wireless Mouse M505
- MX™ 1100 Cordless Laser Mouse
- VX Nano Cordless Laser Mouse
- MX Air™ Rechargeable Cordless Air Mouse

Here are some details from the Logitech website on the technology (**Source:** White paper from <http://www.logitech.com/en-us/mice-pointers/mice/devices/3443>)

In particular, Logitech advanced 2.4 GHz wireless technology hops at 250 times/sec and supports bi-directional data transmission with error correction to maintain a reliable RF link. And Logitech's architecture automatically pairs your peripheral to the provided transceiver that is attached to your computer, while avoiding conflicts with other devices. In other words, when you use a Logitech peripheral with advanced 2.4GHz technology, you can be certain that when you move your mouse or type on your keyboard, your commands will be carried out instantaneously.

Logitech's proprietary wireless protocol is used together with a high-performance RF transceiver. This is a highly integrated, single-chip transceiver that operated in the 2.4 GHz ISM band and is really suited for the most demanding applications. In addition to the technical features described above, this technology also provides the lowest-power RF solution on the market today, translating into significantly longer battery life.

Table 10-1:

Feature	Logitech advanced 2.4 GHz wireless technology	Bluetooth
Range	10m	10-100 m
Bandwidth	2 Mbps bursts	1-3 Mbps bursts
Latency at reconnection	<90 ms	.5-2 seconds
Interference resistance	Best	Best
Battery life	Best	Good
Report rate	125 rpt/s or faster	80 rpt/s
USB interface	FS	FS

Below is a sample of what the spectrum pattern for a Non-Bluetooth Wireless Mouse would look like in a relatively noiseless 2.4GHz spectrum.

Impact on 802.11 WLAN

Since this technology is designed to minimize its interference with WLANs, the impact of having a few of these devices in the spectrum should be low. If there are no frequencies that have low levels of WLAN traffic, the device will choose the least use frequency, which may cause minor disruptions to the WLAN.

Recommended Course of Action

- Ensure that the WLAN network is operating on non-overlapping channels like 1,6, and 11. This will maximize the number of frequencies with little to no WLAN traffic on them.
- If multiple devices of this type exist in the spectrum, begin removing devices until the interference clears up.
- If you have to use your non-Bluetooth wireless mouse along with 802.11b/g WLANs, try to maximize the distance between APs and wireless mice to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offers greater throughput.

Wireless Game Controllers

Wireless game controllers are handheld devices for gaming consoles without wires. Using wireless technology, wireless game controllers allow players to sit virtually anywhere (up to 30 feet away from the game console) in the room, making game play less restrictive.

For better coverage, most wireless game controllers operate on the 2.4-GHz frequency—an unlicensed radio band also used by 802.11b/g WLANs, cordless phones, Bluetooth devices, and microwave ovens, etc. Like the other non-WiFi devices operating in the 2.4-GHz frequency band, wireless game controllers installed in close proximity of an 802.11b/g WLAN can interfere with the normal operation of the WLAN.

Wireless game controllers are available for all major gaming consoles and computers.¹

The following are some of the major brands:

- Sony PlayStation® 2 Wireless Game Controller²
- Microsoft Xbox 360® Wireless Remote Controller

AirMagnet Spectrum XT will identify and list the following game controllers by their brand name: PlayStation 2 and Xbox 360.

RF Spectrum Pattern

Wireless game controllers come in all shapes and sizes. They are widely used in homes and even some businesses settings where the 802.11 WLAN is deployed. Their presence can cause serious performance issues in the WLAN. The figure below shows the RF spectrum pattern of a wireless game controller using the 2.4-GHz frequency band. See Figure 10-16 below.

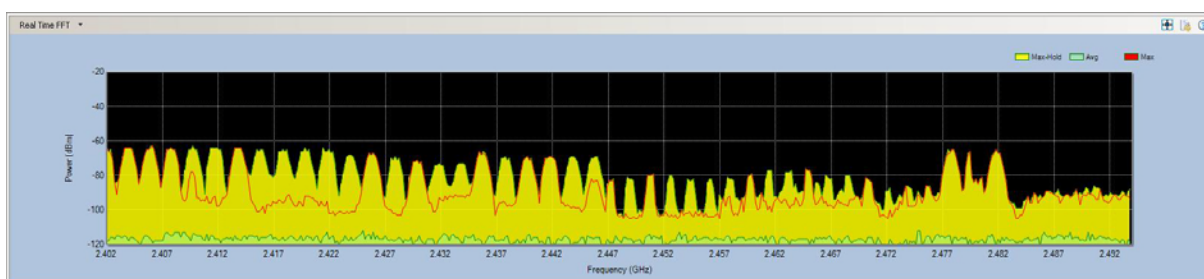


Figure 10-16: RF spectrum pattern of a 2.4-GHz game controller transmitter

1. Nintendo Wii™ and Sony PlayStation 3 are Bluetooth devices and will be detected as Bluetooth interferers.
2. Playstation is a registered trademark of Sony Corporation.

Impact on 802.11b/g WLAN

Because wireless game controllers operate in the same radio frequency as the 802.11b/g WLAN, radio signals from these devices have long been identified as a source of RF interference to 802.11b/g WLANs in homes and businesses where they are used. They can significantly slow down Internet applications such as Web file download and surfing.

Recommended Courses of Action

Once the interfering wireless game controllers are successfully identified, the following actions are recommended to minimize or eliminate the RF interference they cause to the 802.11 WLAN.

- Try to keep a “safe distance” between your 802.11b/g AP and wireless game controller so as to keep interference to the minimum.
- Check the operating channels on the wireless game controller to make sure that they do not overlap with the operating channels of your 802.11b/g network.
- If possible, consider using an 802.11a AP or even upgrading your WLAN to the 802.11n standard.

Frequency-hopping Spread Spectrum devices

Introduction

When the IEEE 802.11 Spec was first ratified, there were two data transmission strategies included: direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS). It was found that, in order to support both strategies, two separate, incompatible sets of transmission technology would have to be developed and maintained. In lieu of this fact, and that 802.11b (which supported DSSS) was more reliable than FHSS, the FHSS strategy was discarded.

When using FHSS, the transmitter shifts the central frequency of a signal several times a second, with each hop taking place in a pseudo-random pattern that both the transmitter and receiver know. In the United States, the FCC mandated at least 75 unique frequencies needed to be used, with a maximum dwell time on each frequency of no more than 400 milliseconds. Limited to speeds of only 1 and 2 Mbps, it was found that not only were FHSS and DSSS incompatible from a communication standpoint, but the FHSS transmissions also interfere with the DSSS communication stream.

RF Spectrum Pattern

While never officially recognized as a ratified 802.11 transmission strategy, there were manufacturers that produced devices with limited interoperability for commercial applications, like Point-of-Sale solutions.

Below is a short list of manufacturers of 802.11 FHSS devices:

- Alvarion
- BreezeCom
- Digital/Cabletron

- Lucent
- Netwave Technologies
- Symbol Technologies
- Proxim Wireless

The figure below shows the RF spectrum pattern of a 2.4GHz 802.11FHSS device.

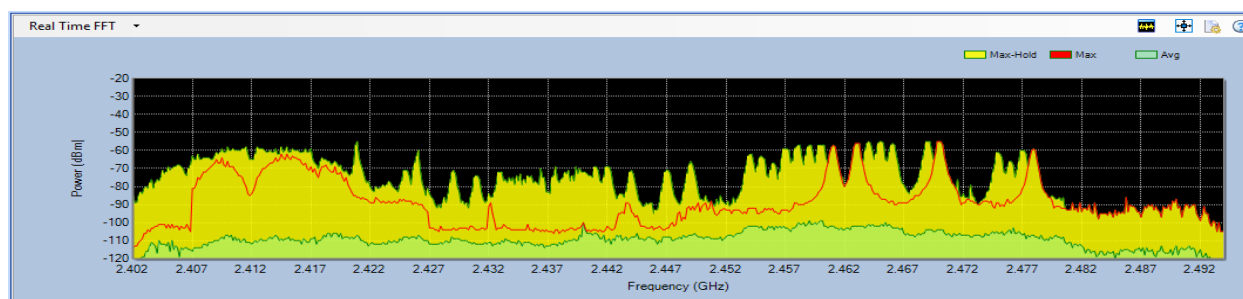


Figure 10-17: Frequency-hopping Spread Spectrum device

Impact on 802.11 WLAN

802.11FHSS devices can have a significant to severe impact on your WLAN. Because these devices hop across the entire band in a semi-random pattern, no 802.11 channel is considered safe from these devices. The actual impact of the 802.11FHSS on your WLAN will depend on the range between the devices, the relative signal levels, and amount of data being transmitted by each network.

Recommended Courses of Action

Once interfering cordless phones are successfully located, you can take the following actions to minimize or eliminate their RF interference to your 802.11b/g or 802.11a WLAN:

- Do not waste your time switching AP channels, because RF signals from digital cordless phones spread over all channels or frequencies in the band they operate. Simply adjusting AP channel is not the solution.
- If you have an 802.11b/g WLAN, avoid or stop using 2.4-GHz FHSS cordless phones. Instead replace them with 5.8-GHz or even old 900-MHz cordless phones which use different radio bands and channels.
- If you have an 802.11a WLAN, avoid or stop using 5-GHz cordless phones. Instead replace them with 2.4-GHz cordless phones.
- If you have an 802.11b/g WLAN and 2.4-GHz cordless phones are a must, try to use those more expensive but less interfering ones which use Digital Spread Spectrum (DSS) technology that offer wider range, better security, with less interference.

- If optimal WLAN performance is not an issue, you may continue use your 2.4-/5-GHz cordless phones along with 802.11b/g or 802.11a WLANs but try to maximize the distance between APs and cordless phone bases to minimize their RF interference between each other.
- Consider upgrading your WLAN to 802.11n standard, which not only provides better RF interference avoidance mechanisms but also offer greater throughput.

WiFi Devices

AirMagnet Spectrum XT not only can detect and present spectrum data of various WiFi devices as it does with non-WiFi devices, but also has the capability to capture various WiFi data about those devices and pinpoint their physical locations in a WiFi network with the help of an AirMagnet-supported wireless network adapter.

This section discusses 802.11 APs. It breaks them up into two groups: 802.11a/g/n APs and 802.11b APs, and talks about their spectrum patterns, impact on the network, and best ways to use them in a wireless network environment.

802.11 a/g/n APs

In general, 802.11a/g/n WLANs offer great advantage over 802.11b WLANs in terms of data rate, signal modulation, etc. The table below provides a brief summary of some key parameters involving all APs built upon different IEEE 802.11 standards.

The 802.11a standard uses Orthogonal Frequency Division Multiplexing (OFDM) modulation which is a more efficient data transmission method than DSSS used by 802.11b, enabling raw data rates up to 54 Mbps. Unfortunately, despite its greater data rates, the 802.11a WLAN never reached the point to replace the 802.11b WLAN due to the fact that it operates in the 5-GHz radio frequency which is incompatible to 802.11b.

The 802.11g standard which uses the same radio frequencies and channels as the 802.11b standard but also supports OFDM offers the best of both worlds: 802.11g WLANs can achieve raw data rates up to 54 Mbps on the same radio frequencies and channels used by 802.11b WLANs. Nowadays, the vast majority of commercial wireless network devices support the 802.11g standard. Much of the WLAN client devices are dual-band supporting both 802.11a and 802.11g.

The emerging 802.11n standard, though not yet ratified, employs several techniques that promise greater throughput, reliability, and stability of WLANs. The key 802.11n technological breakthroughs include (but are not limited to):

- Multiple Input Multiple Output (MIMO) – capable to support up to 4 spatial streams.
- Packet Aggregation – allows transmission bursts of multiple data packets to improve efficiency.
- Channel Bonding (40-MHz channels) – doubles channel width from 20 MHz to 40 MHz to effectively double data rates.
- Improved OFDM – uses a higher maximum code rate and lightly wider bandwidth than the OFDM employed in 802.11a/g standards.

RF Spectrum Pattern

802.11a APs operate in the “regulated” 5-GHz frequency band, meaning that they use radio frequencies that are not used by other commercial wireless products. Unlike 802.11 b/g WLANs which have only three non-overlapping channels, 802.11a WLANs have eight non-overlapping channels to choose from.

Figure 10-18 shows the RF spectrum pattern of an 802.11g/n AP in the 2.402-2.482 GHz frequency range.

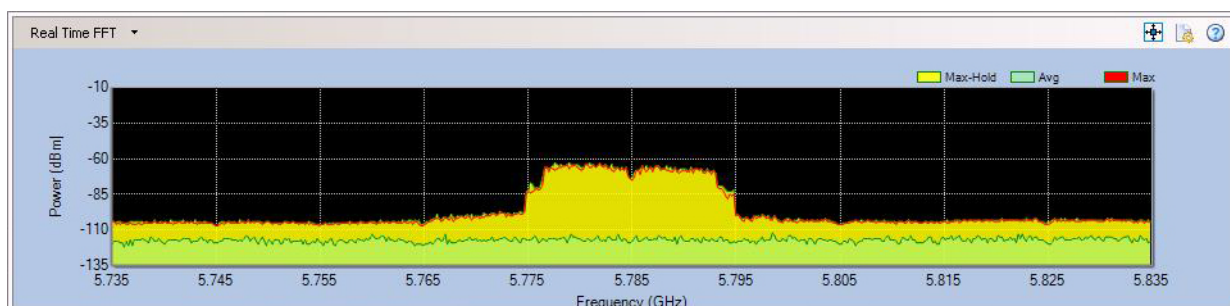


Figure 10-18: RF spectrum pattern of an 802.11g/n AP (OFDM)

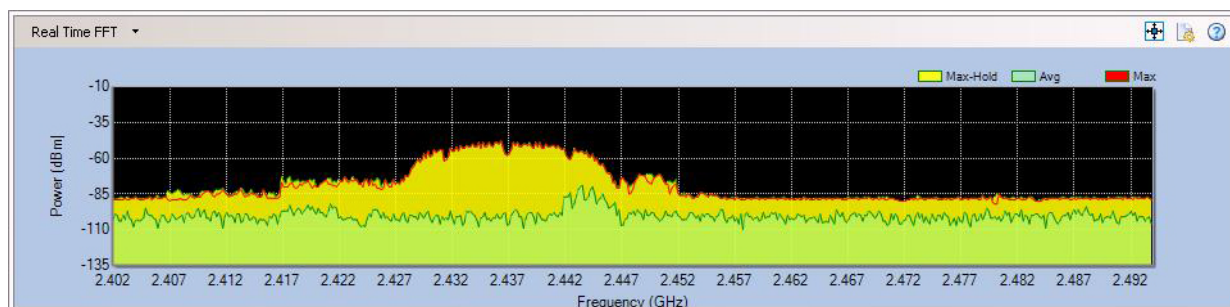


Figure 10-19: RF spectrum pattern of an 802.11g/n AP (CCK)

Impact on WiFi Networks

802.11a uses Orthogonal Frequency-Division Multiplexing (OFDM) signal modulation method, which differs from DSSS signal modulation used by 802.11b WLANs. Since 802.11a WLANs are installed mostly indoors, OFDM is the perfect choice in that it offers better data rates than DSSS and reduces effects of multipath on signal quality and WLAN throughput.

Even though the 802.11a standard helps improve WLAN performance and reduce interference, radio signals from an 802.11a AP can travel a much shorter distance than those of 802.11b/g APs. An 802.11a AP transmitter may cover less than a quarter of the area of a comparable 802.11b AP. Brick walls and other obstructions affect 802.11a WLANs far more than they do to comparable 802.11b/g WLANs.

802.11g APs are backward-compatible with 802.11b APs but offer greater data rates. However, since they operate in the same radio frequencies as their 802.11b counterparts, they are susceptible to RF interference caused by all wireless devices operating in the 2.4-GHz frequency band. See [802.11b APs](#).

802.11n APs, by design, can co-exist with 802.11a APs in the 5-GHz band and 802.11g APs in the 2.4-GHz band since they all use OFDM. The presence of 802.11b devices makes communications a little challenging in the 2.4-GHz band because it cannot understand OFDM which is used by both 802.11b and n standards. In that case, OFDM client devices may have to switch to the older signal modulation (DSSS) to protect their high-rate OFDM transmissions, resulting reduced network efficiency.

Recommended Courses of Action

If you are running an 802.11a/g WLAN, the following action should be taken into consideration when installing and managing your WLAN:

- Since radio signals from 802.11a APs travel a much shorter distance, make sure that you have enough APs to offer adequate WLAN coverage if you are using an 802.11a WLAN.
- If you need more than one AP, make sure to point them to different non-overlapping channels.
- Be aware of other wireless devices that may also be operating in the same radio frequencies and channels as your WLAN APs do. Make sure that your 802.11 WLAN APs use different channels than those used by those competing devices.
- Upgrade your WLAN to the 802.11n standard, if you can.
- When updating to 802.11n, make sure to use “IEEE 802.11n Draft Compliant” hardware devices.

802.11b APs

802.11b APs operate at frequencies in the unlicensed 2.4-GHz Industrial, Medical and Scientific (IMS) band. Because the band is free and used globally, it is crowded with all kinds of 2.4-GHz-compliant commercial products, including:

- WLAN devices (802.11g)
- Cordless phones (digital or analog)
- Bluetooth devices
- Wireless (security) cameras
- Baby Monitors (video and/or audio)
- Microwave ovens

As the number of these devices increases, the 2.4-GHz ISM band is becoming more and more congested. As a result, network performance degradation has become a major issue facing network administrators managing 802.11b/g WLANs. It has long been recognized that the main culprit for WLAN performance degradation is RF interference caused by these competing devices in the 2.4-GHz band. RF interference occurs when two or more RF devices are transmitting at the same frequency at the same time. RF interference causes over-the-air collision which can lead to data corruption and loss.

802.11b APs can operate on one of 13 (11 in the US) channels in the 2.4-GHz ISM band, each being 22 MHz wide and 5 MHz apart. Because each of these channels takes up roughly a quarter of the 2.4-GHz spectrum and adjacent channels tend to interfere with each other, 802.11b WLANs are typically installed using one of three non-overlapping channels, namely Channels 1, 6, and 11.

The table below shows the operating channels for 802.11b WLANs in North America, with Channels 1, 6 and 11 highlighted in grey as non-overlapping channels.

RF Spectrum Pattern

802.11b APs use Direct Sequence Spread Spectrum (DSSS) signal modulation method which is very susceptible to signal multipath. Signal multipath occurs when radio signals are reflected on their way between the transmitter and the receiver. This could happen when radio signals from an AP are blocked by metal furniture, dry walls, and other structural elements common in office buildings. Signal multipath has a huge impact on data quality and WLAN throughput because it causes transmission errors and requires retransmission.

802.11b WLAN APs typically use up to +20 dBm (100mW) transmit power and -80 dBm ~ -90dBm of receive sensitivity. Their bit transfer rate is 11 Mbps (maximum).

Figure 10-20 shows the typical RF pattern of an 802.11b AP.

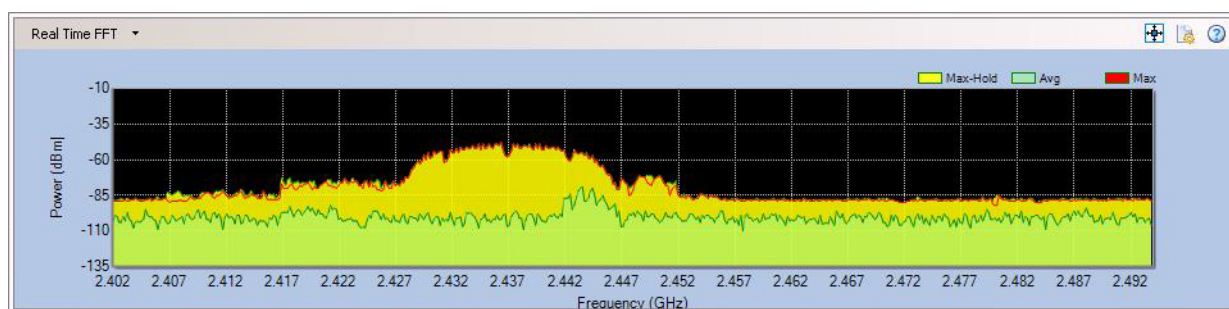


Figure 10-20: RF spectrum pattern of an 802.11b AP

Impact on WiFi Networks

Since 802.11b APs use a fixed bandwidth of 22 MHz in the 2.4-GHz spectrum, the probability of collisions or interference between 802.11b APs or with other 2.4-GHz devices largely depends on the channel they operate. If they are on the same channel or overlapping channels, the probability is high. Otherwise, the chances of collision are low.

Recommended Courses of Action

Since 802.11b/g WLANs are operating in the crowded 2.4-GHz IMS band with so many competing devices (including 802.11b/g devices themselves), the following actions are recommended in order to minimize or eliminate RF interference to 802.11b/g WLANs:

- Prior to installing an 802.11b WLAN, conduct a thorough RF survey of the WLAN site to know all 2.4-GHz devices operating in the WiFi environment and the channels they are using.
- Install 802.11b WLANs by setting the APs to non-overlapping channels 1, 6, and 11, especially when more than one AP is needed.
- Try to avoid the use of HFSS devices in close proximity of an 802.11b WLAN to minimize RF interference.
- If you have more than one 802.11b AP, adjust the transmit power levels on the APs to minimize mutual interference between APs.
- Try to keep WLAN APs at a good physical distance to avoid mutual interference.
- Upgrade your WLAN to 802.11g or n standard

Appendix A: Abbreviations & Acronyms

This section lists the abbreviations and acronyms that appear on AirMagnet Spectrum XT user interface and/or in this User Guide. The full forms of these terms are also given. The definitions of these terms are provided in [Appendix B, "Glossary"](#).

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
a	802.11a
AP	Access Point
Auto	Automatic
Avg	Average
b	802.11b
CH	Channel
CRC	Cyclic Redundancy Check
dBm	Decibels below 1 Milliwatt
FFT	Fast Fourier Transform
g	802.11g
GHz	Gigahertz
IP	Internet Protocol
M	Mbps (Megabit per second)
MAC	Media Access Control
Max	Maximum
MaxHold	Maximum Hold
Misc	Miscellaneous
n	802.11n
RF	Radio Frequency
SSID	Service Set Identity
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

List of Abbreviations and Acronyms

Abbreviation or Acronym	Full Form
WPA	Wireless Protected Access

Appendix B: Glossary

2.4 GHz Band

An option in the Band drop-down list menu, if selected, allows the application to display data captured over the 2.402 GHz ~ 2.482 GHz radio frequency range which covers Channels 1 through 13.

802.1x

A standard designed to enhance 802.11 WLAN security. It provides an authentication framework for WLANs so that users can be authenticated by a central authority. Because the actual algorithm used to determine whether a user is authentic is left open, multiple algorithms are possible.

In a WLAN with 802.1x, when a user requests access to an AP, the AP will force the user (i.e., the client application) into an unauthorized state in which the client can only send an EAP (Extensible Authentication Protocol) start message. The AP, upon receiving the start message, returns an EAP message requesting the user's identity. The client returns the identity, which is then forwarded by the AP to the authentication server. The server uses an algorithm to authenticate the user and then returns either an accept or reject message to the AP. If an accept message was received, the AP then changes the client's state to authorized and normal network traffic starts.

802.11

An IEEE local area network specification that defines the wireless network access link layer. It includes the 802.11 media access control (MAC) sublayer of the Data Link Layer and two sublayers of the Physical (PHY) layer—a frequency-hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. See 802.11a, 802.11b, 802.11e, 802.11g, and 802.11i.

802.11a

A supplement to the IEEE 802.11 wireless LAN (WLAN) specification which defines transmission through the PHY layer based on orthogonal frequency division multiplexing (OFDM), at a frequency of 5 GHz and data rates up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification which defines transmission through the PHY layer based on direct-sequence spread-spectrum (DSSS), at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11g

A supplement to the IEEE 802.11 WLAN specification that defines transmission through the PHY layer based on orthogonal frequency division multiplexing (OFDM), at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A newer standard of WLAN technology designed to significantly improve network throughput over previous standards (i.e., 802.11a, b, and g) by adding multiple-input multiple-output (MIMO) and channel-bonding/40-MHz operation to the physical (PHY) layer, and frame aggregation to the MAC layer. The 802.11n standard promises data rates up to 600 Mbps.

AP (Access Point)

A hardware device that links or bridges wireless stations to a wired network. APs serve to centralize all wireless stations on a LAN in a so-called “infrastructure” mode. They are commonly used in large office buildings or public places like airports to form one wireless local area network (WLAN) that covers a large area. Each AP typically supports 255 wireless stations. Also known as wireless access point or WAP.

Authentication

Any security measure adopted to establish the validity of a transmission, message, or originator, or a process for verifying a party’s authorization to receive certain information.

Band

Refers to the radio band which is a section of the spectrum of the 802.11 radio communication frequencies in which 802.11 radio channels are allocated. AirMagnet Spectrum XT provides four basic band segments (i.e., 2.4 GHz, 5 GHz Lower, 5 GHz Middle, and 5 GHz Upper) whose ranges are based upon a wireless network adapter's capability and determined by the regional settings burned into the adapter's EEPROM.

Bandwidth

In computer networking, the term refers to the data rate supported by a network connection or interface. It is the overall capacity of a connection. The greater the capacity, the greater the performance, though the overall network performance may also be affected by factors such as latency, usage, etc.

Broadcast

The process of sending the same data to all stations on the network. See multicast and unicast.

Channel

A radio frequency or band of frequencies assigned to a specific country or region of the world by an international agreement. For instance, 802.11b is made up of 13 unlicensed channels (i.e., Channels 1-13) in the 2.4 GHz band (i.e., from 2402 MHz to 2482 MHz in 5 MHz steps).

Channel Duty Cycle Graph

A graph that displays the current percentage of time that the average power in the channel is greater than -20 dBm above the noise floor.

Channel Occupancy

The state of occupancy of all available channels. It provides a simple and straightforward way for the user to know which channels are in use and which channels they should choose if they want to select a channel for better signal quality.

Channel Power Graph

A graph that displays the maximum and/or average power level on a channel. AirMagnet Spectrum XT shows two types of channel power: Envelop vs. Integrated. The former refers to the maximum or peak energy level at a particular frequency. In this case, the height of the bar chart represents the highest power level that has been reached at a particular frequency within a channel; the latter refers to the total summation of power that has been observed over the entire frequency range.

Color Scale

A setting in the Spectrum Density and Spectrogram graph that uses blue and red as two border colors and fills a smooth gradient in between. It helps the user to visualize the changes in power levels across the spectrum, with blue denoting the Minimum and red the Maximum. See Spectrum Density and/or Spectrogram graph.

Color Scale Mode

A setting in the Spectrum Density graph which allows the user to choose the way the Color Scale is configured. Choose Auto to let the application configure the Minimum Percentage and Maximum Percentage; select Manual to set these two values manually.

Crash

Any critical failure in a computer, network device, or software application that runs on such devices. When a crash occurs, a computer may freeze or hang indefinitely. A crash could occur without warning. The user may have to power down and then restart the computer or network device in order to recover from a crash.

CRC (Cyclical Redundancy Check)

An error-checking technique used to ensure the accuracy of data transmitted over the network. Each transmitted message is broken down into predetermined lengths which are then divided by a fixed divisor. The remainder of the calculation is appended onto and sent with the message. Upon receiving the message, the receiving station recalculates the remainder. An error is detected when it does not match the transmitted remainder.

Data Rate

Refers to the speed (in Mbps) at which data are transmitted over a channel.

dBm (Decibels below 1 Milliwatt)

Decibels relative to 1mw.

Driver

Also called device driver or software driver, is a computer program specifically written for the wireless network adapter to enable it to interact with higher-level computer programs (e.g., an operating system, applications, etc.).

Encrypted

A variable that may show up in the Security column in the WiFi Device graph. It means that the application has determined that packets transmitted by a certain device are encrypted even though it cannot determine the specific security mechanism that is being used.

Encryption

The reversible transformation of data from the original to a difficult-to-interpret format (the encrypted) as a way to protect their confidentiality, integrity and sometimes authenticity. It involves the use of an encryption algorithm and one or more encryption keys.

FCC (Federal Communications Commission)

A United States federal government agency that regulates communications in the country.

FFT Graph

The FFT (Fast Fourier Transform) graph displays the current, average, and maximum power readings in dBm in the selected spectrum bands or channels.

First Frame Time

The time when the first frame was detected being transmitted from a device in the wireless environment.

Frame

In communications, a fixed block of data transmitted as a single entity over the network.

IEEE (Institute of Electrical and Electronic Engineers)

A non-profit engineering organization in the United States that develops, reviews, and promotes standards within the electronics and computer industries.

Interference

In wireless networking, the disturbance that results when radio signals from different APs collide in the airwave.

IP (Internet Protocol) address

A 32-bit unique string of numerical characters used to identify a networked computer, printer, or any other device.

LAN (Local Area Network)

A short-distance network that joins a group of computers together, usually within the same building. Using a network hub as a wiring point, data can be sent from one computer to another over the network.

Last Frame Time

The time when the last frame was detected being transmitted from a device in the wireless environment.

MAC (Media Access Control) address

A unique, 48-bit number assigned to each IP network adapter. It is written in a sequence of 12 hexadecimal digits (e.g., 46:2F:0B:19:11:CB) . Each MAC address is uniquely set by the network device manufacturer and is sometimes called the device's "physical addresses". The first six hexadecimal digits of an MAC address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number.

Marker Type

A settings in the Real-Time FFT graph that becomes available once the Enable Marker is selected in the Market Settings. There are two options for Marker Type: Single vs. Delta. Markers are used to identify the data point or points of interest in the Real-Time FFT and provides brief information about them.

Marker Settings

Marker Settings refer to the parameters used in the configuration of the Real-Time FFT graph. See Marker Type and Spectrum Type.

Maximum Percentage

A parameter used in the configuration of the Spectrum Density graph. It can any value greater than the Minimum Percentage but equal to or less than 100. *See Minimum Percentage.*

Media

Refers to the 802.11 protocol or protocols, which include 802.11a, b, g, and n, used by wireless network or device.

Minimum Percentage

A parameter used in the configuration of the Spectrum Density graph. It can any value less than the Minimum Percentage but equal to or greater than 0. *See Maximum Percentage.*

Minimum Power

A parameter in the configuration of Real-Time FFT, Spectrum Density, and Channel Power graphs. By default, it is -120 dBm, but the user can set it to any value as long as it is less than the Peak Power but equal to or greater than -140 dBm. *See Peak Power.*

Mixed

A option in the Band drop-down list menu, if selected, allows the application to display data captured across all 802.11 radio spectrums and channels. *See also 2.4 GHz, 5 GHz Lower, 5 GHz Middle, and 5 GHz Upper.*

Modulated Interference

Interference from a device (to a channel) caused by modulated spectrum (i.e., within the device's operating channel width).

Multicast

The process of sending a single message to multiple destinations simultaneously. It is a one-to-many transmission similar to broadcasting, except that multicasting means transmission to specific groups, whereas broadcasting implies sending to everybody. Multicasting can save considerable bandwidth when sending large volumes of data because the bulk of the data is transmitted once from the source through major backbones and are multiplied, or distributed out, at switching points closer to the recipients. In a unicast system, the data is replicated entirely to each recipient. Compare unicast.

Noise

In wireless networking, any radio signal that does not convey useful data. *See Noise Floor.*

Noise Floor

Refers to the natural interference in a wireless network environment.

Open

A variable in the Security column of the WiFi Devices graph. It means that the application determines that no security mechanism is used on a certain device based on packets transmitted from that device.

Peak Power

A setting used in the configuration of Real-Time FFT, Spectrum Density, and Channel Power graphs. By default, the Real Power is -20 dBm, but the user can change it to any value greater than the Minimum Power but equal to or 1

Phone

Refers to VoFi (Voice over Wi-Fi) phones.

RSSI (Received Signal Strength Indicator)

A measurement of power (in dBm) in the radio signal received in a Wi-Fi environment. *See Signal Strength.*

Service Set Identifier (SSID)

A unique name that identifies a wireless network or a network subset. It is used by every device connected to the network or that part of the network to identify itself as part of the family when accessing the network or verifying the origin of a data packet it is transmitting.

Signal

In wireless networking, any electrical pulse or frequency that carries meaningful data. *See RSSI.*

Spectrum Density Graph

A graph that shows the “popularity” of a particular frequency/power reading over time in the radio spectrum.

Spectrum Type (Current, Average, Maximum)

Refers to the type of spectrum data presented in the Real-Time FFT graph. AirMagnet Spectrum XT can show three types of spectrum data:

- Current – The up-to-the-minute power readings being recorded.
- Average – The average historical power readings recorded since the beginning of the session.
- Maximum – The highest power readings that have been recorded since the session began.

Spectrogram Graph

Provides another way to present the same data as shown in the Real-Time FFT graph. It shows changes in the spectrum over a period of time and identifies any shift in frequency use and the duration of such shifts.

SSID (Service Set Identifier)

A unique name given to a WLAN and shared by all devices, e.g., APs, stations, etc. operating in the WLAN.

Start Channel

A setting in the configuration of the Channel Power and Channel Duty Cycle graphs. It refers to the first radio channel in the range of channels shown in the graph. *See Stop Channel.*

Start Frequency

A parameter used in the configuration of Real-Time FFT, Spectrum Density, and Spectrogram graphs. It is the value of radio frequency at the lower end of the spectrum band in these graphs. *See Stop Frequency.*

Station

In wireless networking, any device with a MAC address and a physical layer (PHY) interface to the wireless medium that comply with the IEEE 802.11 standard, e.g., a laptop, PDA, etc.

Stop Channel

A parameter used in the configuration of the Channel Power and Channel Duty Cycle graphs. It refers to the last radio channel in the range of channels shown in the graph. *See Start Channel.*

Stop Frequency

A parameter used in the configuration of the Real-Time FFT, Spectrum Density, and Spectrogram graphs. It is the value of radio frequency at the upper end of the spectrum band in these graphs. *See Start Frequency.*

Unicast

The process of sending duplicates of the same message to multiple destinations on the network. In unicast, even though multiple users might request the same data from the same server at the same time, duplicate data streams are transmitted, one to each destination. Compare multicast.

Unknown

A variable in the Security column of the WiFi Device graph. It means that the application is unable to determine whether any security mechanism is used on a certain device based on packets transmitted from that device.

Unmodulated Interference

Interference caused by signal “bleed over” outside the modulated spectrum of a device.

WEP (Wired-Equivalent Privacy)

A security protocol within the IEEE 802.11 standard that provides a WLAN with a *minimum* level of security and privacy comparable to that of a typical wired LAN. WEP encrypts data transmitted over the WLAN to protect vulnerable connection between APs and stations. However, since WEP regulates WLAN access based on a device’s MAC address which is relatively easy to be sniffed out and stolen, it offers limited security to a WLAN.

Wireless Network Adapter

A hardware device that interfaces a station (e.g., a computer) to a network. Modern network adapter hardware comes in many forms, such as PCI Ethernet cards, PCMCIA devices, or USB devices. Some laptop computers even come with integrated wireless network adapters pre-installed on them in the form of circuit chips. Operating systems support network adapters through a piece of software known as “device driver”, which enables application software to communicate with the adapter. Some network adapters are software packages that simulate the function of a network adapter. Also known as wireless network card, WiFi card.

WLAN (Wireless Local Area Network)

A local area network (LAN) to which wireless users (stations) can connect and communicate via high-frequency radio waves rather than copper wires.

WPA (Wi-Fi Protected Access)

A security protocol for the IEEE 802.11 standard designed to overcome the security vulnerabilities of WEP. WPA operates in either WPA-Personal mode (aka Pre-Shared Key) or WPA-Enterprise mode (aka RADIUS or WPA-802.1x). In WPA-Personal mode, a pre-shared key is used for authentication. In WPA-Enterprise mode, which is more difficult to configure, the 802.1x RADIUS servers and an Extensible Authentication Protocol (EAP) are used for authentication. The enhanced WPA2 uses Advanced Encryption Standard (AES) instead of Temporal Key Integrity Protocol (TKIP) to provide stronger encryption mechanism.

WPA-Personal

See WPA.

WPA-Enterprise

See WPA.

WPA2

Short for Wi-Fi Protected Access 2, which is a follow-on security method to WPA for the WLAN. It provides stronger data security and network access control, assuring Wi-Fi users that only authorized users can access their WLANs. Based on the IEEE 802.11i standard, WPA2 meets the stringent US government-grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication.

WPA2 comes in two flavors: WPA2-Personal and WPA2-Enterprise. The former is used to prevent unauthorized network access by utilizing a set-up password, whereas the latter verifies network users through a designated authentication server.

WPA2 is backward compatible with WPA.

WPA2-Personal

See WPA2.

WPA2-Enterprise

See WPA2.

Index

Numerics

1st Max 93
2nd Max 93
3rd Max 93
802.11 radio bands 29

A

AirMedic CD 11
AirMedic menus and tools 29
AirMedic software CD 11
Alert Settings 38
Analog Cordless Phones 119
AP Name 92
AP signal curves 68
AP Signal Strength 3, 92
Auto 70
AutoHide 92, 95
average power 75

B

Baby Monitors 119
Band 116
bluetooth 24
Bluetooth Devices 119
Broadcast 98

C

CD 11
CD-ROM drive 11
Channel 38
Channel by Address graph 3
Channel by Media graph 3
Channel by Speed graph 3
Channel Duty Cycle 83
Channel Duty Cycle graph 2
Channel Occupancy 94
Channel Occupancy graph 3
Channel Power 73
Channel Power graph 2

Channel Power Type 76
channel power types 74
channel scan indicator 27
Channel Summary 24
Channel Usage 26
Channel Utilization 99
Channel Utilization graph 3
channels 30
Channels by Address 97
Channels by Media 96
Channels by Speed 95
Chart Configuration button 27
Color Scale Mode 70
configure 69, 72, 77, 84
configure Real Time FFT 65
copy and paste a graph 48
copy-and-paste 5
create a custom view 46
custom view 46

D

default graph window 26
delete a custom view 47
Delta marker 66
Device Description 109
Device Details 106
Device List 25
Device Pattern 108
Device/MAC 91
DFS 113
DFS2 113
DFS-3 113
DFSA 113
Digital Cordless Phones 119
Display Options 36, 37
Duty Cycle 38
Dynamic Frequency Selection (DFS) 113

E

Easy View list menu 45

Envelope 76
ETSI 115
Event Log 106
Event Spectrogram 2
Export (radar) 116
external wireless network adapter 27, 89

F

Fast Fourier Transformation 62
FFT Channel Duty Cycle Overlay 64
FFT Graph Channel Duty Cycle 64
Fid Device 105
Find Device 4
Find Device tool 108
First Frame Time 91
fluorescent light 24
Frequency 38

G

general WiFi and spectrum parameters 33
graph window 26
graphs 26

H

help button 27

I

image file 5
image formats 5, 49, 50
Installing 11
instant playback 4
Integrated 76

L

Last Frame Time 92
License Agreement 13
live Internet access 11

M

MAC Address 91
Main Features 1
main features 1

major UI components 19
Manual 70
marker 66
Marker Type 66
maximum percentage 70, 78, 85, 86
maximum power 73, 75
Microwave Ovens 119
microwave ovens 24
minimum percentage 70, 78, 85, 86
minimum power 67, 70, 73, 76
Multicast 98

N

noise level 91
Non-WiFi Devices 2
non-WiFi devices 24

P

pausing and resuming live capture 31
peak power 67, 70, 76
Period 116
Product Overview 1
product support 16

R

Radar Class Type 115
Radar Detection Tool 113
radio band 30
radio frequency 30
Real-Time FFT 62
Real-Time FFT graph 1
record live capture data 4
register 16
Registering 11
reinstall 15
replay recorded data 5
Report 50
resetting collected data 33
right-click menus 5

S

save a graph 49

- save current view 47
- save recorded data 5
- Scan Time 116
- security 91
- serial key 11, 14
- serial number 11, 14
- Settings (radar) 115
- Show Area Fill 65
- signal strength 91
- Signal Strength Gauge 109
- Single maker 66
- Software Installation 11
- software installation 11
- software license file 13
- Spectrogram 71
- Spectrogram graph 1
- spectrum analysis 1
- Spectrum Density 67
- Spectrum Density graph 1
- spectrum graphs 1, 61
- Spectrum Type 67
- Spectrum-WiFi Summary 24
- SSID 91
- Start Channel 76, 78
- start frequency 67, 70, 73
- Start Scan 116
- Stop Channel 76, 78
- stop frequency 67, 70, 73
- Supported Wi-Fi Cards 8
- supported wireless network adapter 8
- system configuration 33

- system parameters 33
- System Requirements 6
- system requirements 6

T

- technical support 11
- TELEC 115
- tip screen 93
- tool tip 67
- toolbar 21
- Top 10 Active APs' Retry/CRC 101
- Top 10 Active APs' Retry/CRC graph 3
- Top 10 APs by Speed 3, 100

U

- Unicast 98
- user interface 19

V

- View Typ 72

W

- WiFi 3
- WiFi Devices 90
- WiFi devices 24
- WiFi Devices graph 3
- WiFi driver 36
- WiFi graphs 2, 89
- wireless adapters 8
- wireless network adapter 1

